secunet

Annual Financial Statements 2025

secunet.com

Fundamentals of the Group

This Management Report combines the Management Report of secunet Security Networks AG (hereinafter "secunet AG") and the management report of the secunet Group (hereinafter "secunet"). This is done because the risks and opportunities of the parent company, as well as its anticipated development and key research and development activities, are inextricably linked to the Group. Therefore, the Management report of secunet AG is consistent with the situation of the secunet Group.

Business model

secunet is one of Germany's leading cybersecurity companies. In an increasingly interconnected world, the company combines products and consulting services to create resilient digital infrastructures and provide the highest possible level of protection for data, applications, and digital identities. A key component of its portfolio is network components featuring advanced encryption technologies, certified by the German Federal Office for Information Security (BSI) up to the highest national security level. secunet is an IT security partner of the Federal Republic of Germany and a partner of the Alliance for Cyber Security.

secunet's business covers the entire value chain, from analysis and design through development to integration, operation, maintenance, and support of solutions. By extensively utilizing open-source software and employing a multitude of coordinated security mechanisms, flexible, scalable, and highly secure solutions are realized. These are typically tailored to specific application scenarios in industries with particularly stringent information security requirements. This includes, above all, the public sector, encompassing national and international governments, ministries, and agencies, as well as quasi-governmental organizations. The German Armed Forces and defense organizations, along with security agencies such as police and border patrols, are also key clients. Furthermore, the company addresses sectors with specific IT security needs, such as healthcare and industry.

Group organization

Legal group structure

secunet Security Networks AG is the parent company of the secunet Group. The company is headquartered in Essen, Germany. It acts as the strategic and financial management body for the Group and encompasses the majority of its operational business units. Furthermore, Group-wide central functions such as finance, accounting, controlling, internal audit, legal, compliance, human resources, IT, investor relations, sustainability, and corporate communications are organized centrally and are the direct responsibility of the Management Board.

secunet AG holds all shares in its subsidiaries SysEleven GmbH (based in Berlin), secunet International GmbH (Munich), and stashcat GmbH (Hanover). The Group also includes the non-operating secunet Inc. (Texas/USA) and the non-operational and deconsolidated secustack GmbH i.L. (Dresden).

secunet International GmbH consolidates the international sales activities for the SINA product family, which were previously handled by secunet International GmbH & Co. KG. secunet International GmbH emerged as the legal successor of secunet International GmbH & Co. KG and secunet International Management GmbH, after the following reorganization measures: By shareholder resolution of February 28, 2025, the Articles of Association of finally safe GmbH were amended, resulting in its renaming as "secunet International GmbH" and the relocation of its registered office from Essen to Munich. Subsequent corporate restructuring measures led to the dissolution of secunet International GmbH & Co. KG and secunet International Management GmbH without liquidation, and their entire assets were transferred to secunet International GmbH by way of universal succession as of September 1, 2025.

SysEleven GmbH is a German provider of cloud infrastructure, cloud services, managed services, and managed Kubernetes. The company operates its own open-source-based cloud infrastructure with ISO 27001-certified data center locations in Germany (Infrastructure as a Service) and offers MetaKube, a platform for the efficient management and optimization of computing, storage, and network resources based on Kubernetes (Managed Kubernetes). Since the beginning of the year, the company's sales activities have been handled by secunet AG.

stashcat GmbH offers a business messenger that enables secure and GDPR-compliant messaging and includes additional security-optimized collaboration and video conferencing functions.

Giesecke+Devrient GmbH, based in Munich, is the majority shareholder of secunet AG with a direct stake of 75.12%. The owner-managed Giesecke+Devrient GmbH, as a strategic holding company, unites its affiliated companies, including secunet AG. The group is internationally oriented and active in the field of banknote and security printing, as well as the development and production of security paper and banknote processing systems. Furthermore, the group develops and manufactures magnetic stripe and chip cards, primarily for the telecommunications, banking, and healthcare sectors.

Group management

As a German stock corporation, secunet AG has a dual management system consisting of a Management Board and a Supervisory Board. The Management Board manages the company independently and is advised and supervised by the Supervisory Board.

For further information on the composition and distribution of responsibilities of the Management Board and Supervisory Board, please refer to the Corporate Governance Statement, which is part of this report and available on the corporate website. This statement also includes the declaration of conformity pursuant to Section 161 of the German Stock Corporation Act (AktG).

Locations

At the end of 2025, the secunet Group had thirteen locations in Germany.

Business activities

The secunet Group's operating business is divided into two segments: the Public Sector and the Business Sector. In its financial reporting, secunet reports on operational business performance through these segments, in addition to the overall view of the Group. Within each segment, the organization is process-oriented and aims to provide optimal service to the respective markets and customers.

Public sector

The Public Sector segment serves public sector clients, including national and international governments, ministries and agencies, as well as quasi-governmental organizations. This client group also includes the German Armed Forces and defense organizations, as well as security agencies such as police and border guards.

A key component of the product range is the IP-based cryptosystem SINA ("Secure Inter-Network Architecture"), developed in cooperation with the German Federal Office for Information Security (BSI). SINA protects electronic information from unauthorized access and enables the secure processing, storage, and transmission of classified information via the internet. With BSI approvals up to the highest national security classification of SECRET, SINA meets maximum security standards.

The SINA product family comprises a constantly growing number of modular components such as clients, gateways, servers, and software tools. These components are used to secure a wide variety of application scenarios. Special SINA components are offered for high-security military and government networks, which place particularly high demands on data security and equipment resilience. These components are based on a hardened hardware platform and are designed for extreme operating conditions.

The Public Sector segment also encompasses activities in the areas of digital identities and biometrics. The offering includes solutions for personal identification and user authentication on web portals, as well as biometric data capture and verification in connection with official identity documents. This also

includes automated border control systems that ensure a smooth and secure flow of passengers at airports and other border control points.

The business activities of the subsidiaries SysEleven GmbH and stashcat GmbH are integrated into the Public Sector segment. In addition to the product range, the segment also encompasses a broad spectrum of consulting services, ranging from security analyses (known as penetration testing) and security consulting (for example, for security policies and their implementation) to support in certification processes.

Business sector

The Business Sector segment addresses two markets in the private sector: healthcare and industry.

In the healthcare market, secunet targets its services at medical providers, including physicians, hospitals, and pharmacies. The core of its offering lies in providing various connectors. These connectors offer secure access to the telematics infrastructure (TI) and provide interfaces to applications such as the electronic patient record (EPR) and the electronic prescription (ePrescription). Additionally, the connectors perform crucial security functions, such as encrypting and signing medical documents. This ensures the secure transmission and processing of sensitive health data within digital healthcare applications.

For industry, secunet offers solutions for secure edge computing as well as early warning systems for the prevention and detection of cyberattacks. The focus is particularly on manufacturing companies with high security requirements. Critical infrastructures (KRITIS) are also addressed, meaning organizations and facilities of vital importance to the functioning of society, including those in the energy, transport, water, finance, and insurance sectors.

As in the Public Sector segment, the Business Sector segment also encompasses a wide range of consulting services.

International business

In both segments, the primary geographical focus of sales is in Germany. secunet's international sales activities concentrate on the countries of the European Union, EU organizations, defense and space agencies (including organizations such as NATO), and the Middle East.

Procurement

The secunet Group does not own any manufacturing facilities. For the value creation and production of its hardware products, secunet collaborates with a wide range of manufacturing partners. This includes both standard products from computer manufacturers, which are subsequently enhanced with security features, and specialized products manufactured to secunet's specifications. For particularly security-critical components, secunet prioritizes partners from Germany or the European Union. When procuring software components used in its products, secunet focuses primarily on open source software – software whose source code is freely available and, depending on the underlying license, may be used commercially.

The secunet Group places particular importance on ensuring that fundamental labor, social, and environmental standards are upheld in the production and transport of the products it distributes. The company respects and supports the principles of the International Labour Organization (ILO), the Supply Chain Due Diligence Act, and the UN Global Compact. secunet communicates its code of conduct regarding human rights, working conditions, environmental protection, and legally compliant and ethical business practices to its suppliers. These principles of conduct are defined in the Code of Conduct for Suppliers and Business Partners, which was updated in 2022 and is binding for all suppliers and business partners. Through this Code, secunet obligates its partners to align themselves with our principles of conduct, to comply with them and pass them on in their supply chain. This is an essential building block for fulfilling social, environmental, and economic responsibility in the supply chain.

Management system and key performance indicators

Internal Group management system

The secunet Group and secunet AG are managed in accordance with the long-term strategy and short- and medium-term objectives. The Management Board shares responsibility for overall planning and for implementing the formulated objectives within the framework of strategic corporate development.

The Management Board primarily uses financial management and performance indicators to assess current business performance and make decisions regarding future strategies and investments. As part of the annual strategy process, an internal plan for the medium term and a financial forecast for the coming year are developed. In parallel, a forecast for the current financial year is regularly prepared based on current business performance. The Management Board monitors goal achievement through a comparison of planned versus actual results and by means of the forecasts. Furthermore, progress toward achieving the strategic targets is regularly reviewed and analyzed at meetings of the Management Board.

Financial management and performance indicators are also used in financial reporting. A detailed description of their development can therefore be found in the "Business Report" section.

The company is not managed exclusively on the basis of financial indicators, but also takes into account non-financial performance indicators as well as industry- and company-specific early indicators.

Key financial performance indicators

The most important financial indicators for corporate management and financial reporting are revenue, earnings before interest, taxes, depreciation, and amortization (EBITDA), and earnings before interest and taxes (EBIT). EBIT represents the net income before interest income, interest expenses or financial income, income from investments (especially in the context of HGB-compliant financial statements), and taxes. It provides a representation of operating profit without the influence of effects from internationally inconsistent tax systems and varying financing activities.

Key financial performance indicators are recorded and monitored both at the group level and in the individual segments. They form the basis for management processes and decision-making at the strategic and operational levels, including, for example, investment and acquisition decisions.

The remuneration of the Management Board members includes a variable component that depends on the achievement of targets for financial performance indicators. This is described in detail in the separate "Remuneration Report pursuant to Section 162 AktG".

Other financial performance indicators

For the purpose of evaluating economic performance, the secunet Group uses additional financial performance indicators in both corporate management and financial reporting. Unlike the previously mentioned indicators, these financial performance indicators are only of secondary importance. Therefore, no forecasts are provided for these indicators.

These key performance indicators include, in particular, gross profit and operating expenses. Gross profit, derived from the difference between revenue and cost of sales, serves as an indicator of the company's value creation. Operating expenses comprise expenditures incurred in the course of normal business operations. A distinction is made between selling expenses, research and development costs, and general administrative costs.

Key non-financial performance indicators

In addition to financial performance indicators, the Group is also managed using non-financial indicators, which are secondary to the financial performance indicators. The compensation of the Management Board members includes a variable component that depends on the achievement of targets for certain non-financial performance indicators. These are various sustainability and ESG targets (usually three) that the Supervisory Board determines annually in connection with setting the targets for variable Management Board compensation. In 2025, these included (i) increasing customer satisfaction compared to the reference group through a Net Promoter Score survey, (ii) achieving a certain percentage of women in management positions within the secunet Group as a target for promoting women, and (iii) reducing CO_2 emissions, measured in tons per employee.

Detailed descriptions of the aforementioned key figures can be found in the separate "Remuneration Report pursuant to Section 162 AktG".

Sector and company-specific early indicators

According to the Management Board, the key company-specific early indicators are incoming orders and the order book. These figures are recorded monthly and serve as an indication of expected capacity utilization as well as anticipated revenue and earnings development.

Furthermore, in order to gain an overview of market conditions, management continuously monitors and analyzes statistics and forecasts on general economic developments as well as the dynamics of the IT and IT security markets.

Research and development

The research and development activities of the secunet Group, secunet AG, and SysEleven GmbH aim to identify technological trends early and address them proactively. This is intended to optimally support the achievement of the company's strategic objectives. The focus is on developing new products, opening up new markets, and acquiring new customers. These research and development activities are conducted both for internal purposes and within the framework of individual customer projects.

Innovation management

Strategically, secunet bases its innovation efforts on three pillars:

- Promoting a culture of innovation by incentivizing new developments, as well as regular and intensive internal professional exchange and the development of an infrastructure for knowledge management;
- Cooperations and partnerships with customers, suppliers, universities and associations to achieve synergies in research and development;
- Organizational pooling of expertise in product management, accompanying developments from innovation management to the creation of market-ready products.

Employees of the secunet Group are members of numerous national and international standardization and regulatory bodies. This active participation enables the early evaluation, recognition, and implementation of IT innovations. The Management Board believes that this not only fosters the valuable exchange of expertise but also contributes to the continuous professional development of its own workforce.

Economic report

Macroeconomic environment

Due to its high sales share, Germany is the most important sales market for the secunet Group.

The German economy turned the corner in 2025 after two years of recession and experienced slight growth. According to the Federal Statistical Office, gross domestic product (GDP) rose by 0.2 percent, primarily due to increased consumer spending by private households and the government. In contrast, exports declined again. The export sector faced headwinds from higher US tariffs, the appreciation of the euro, and increased competition from China.

The inflation rate in Germany averaged +2.2% in 2025. After the high rates of previous years, the rise in consumer prices thus stabilized at a level close to the target value of the European Central Bank (ECB), but remained significant, particularly in the services sector.

Sector-specific environment

Information and communication technology (ICT) market

In addition to the general economic development in Germany, the overall market for information technology and telecommunications (ICT) forms an essential framework and basis for comparison for assessing the economic development of the secunet Group.

Last year, spending on information technology and telecommunications (ICT) increased by 3.9% to €234.8 billion. Contrary to the overall economic trend, the business climate in the digital economy developed positively. A key factor in this development was the information technology (IT) market, which is particularly relevant for the secunet Group and grew at an above-average rate of 5.2% in 2025. This market encompasses IT hardware, software, and IT services. Software spending saw the strongest growth in this segment, increasing by 9.5% to €52.9 billion. With a rising growth rate of 3.8%, IT hardware, at €55.2 billion, maintained its position as the most important part of the IT market, followed by IT services, whose spending increased by 2.7% to €52.5 billion (Source: Bitkom, January 2026).

IT security market

The economic environment for companies in the cybersecurity sector was therefore very robust in 2025, within an otherwise stagnant German economy. While the gross domestic product rose only slightly, the IT security market decoupled from the general economic slowdown and solidified its role as a growth market. This dynamic was primarily driven by a combination of increased regulatory requirements, an increasingly challenging global threat landscape, and the pressing demand for technological upgrades through artificial intelligence.

Business risk of cyberattacks

Cyberattacks continue to pose a significant threat to society and the economy. The impact of such attacks extends far beyond financial damage and affects critical infrastructure such as hospitals, power plants, airports, and transportation systems.

The business risk posed by cyberattacks will have reached a new dimension by 2025, transforming from a purely technical IT problem into a central corporate risk with existential implications. The threat landscape is now characterized by a significant professionalization of attackers, who use generative artificial intelligence to conduct automated and highly personalized attacks on an industrial scale. According to Bitkom, the damage to the German economy amounted to approximately €289 billion last year, representing an increase of 8.5% compared to the previous year.

To withstand the threat landscape, German companies have fundamentally transformed their defense strategies. The modern bulwark is no longer based solely on isolated technical solutions, but on a holistic ecosystem encompassing technology, organization, and corporate culture. A key element is the transition to a zero-trust architecture, where, according to the principle of "never trust, always verify," all access within and outside the network is strictly controlled.

Increasing regulation

The topic of IT security is receiving additional support through increased regulation. This contributes to cybersecurity being understood not merely as a technical necessity, but as a fundamental business requirement. New legal regulations and international standards promote robust security structures and compel companies and the public sector to regularly review and adapt their protective measures.

The year 2025 saw the full implementation of the EU's NIS2 directive and the Cyber Resilience Act (CRA). These regulations extend security requirements to thousands of small and medium-sized enterprises (SMEs) that were not previously considered "critical infrastructure". For cybersecurity providers, this could mean increased demand for compliance consulting, audits, and technological solutions for attack detection. Companies may be forced to invest more heavily to avoid fines and ensure their supply chain resilience.

These regulatory measures motivate companies and governments to invest more heavily in IT security to strengthen their resilience against digital threats. The clear legal anchoring fosters trust and leads to cybersecurity being recognized as an integral part of corporate strategy.

Business performance in 2025

Business performance of the secunet Group

In financial year 2025, the secunet Group generated sales revenue of €458.8 million (previous year: €406.4 million, 2025 forecast: €425 million). This represents an increase of 12.9%. EBIT reached €51.6 million, compared to €42.5 million in the previous year, an increase of 21.5%. This corresponds to an EBIT margin of 11.3% (previous year: 10.5%, 2025 forecast: 9.5–11.5%). EBITDA also increased further to €74.9 million, exceeding the previous year's figure by 24.2% (previous year: €60.3 million). The EBITDA margin rose accordingly to 16.3%, compared to 14.8% in the previous year (2025 forecast: 14.5–16.5%). As in previous years, business development in 2025 was also characterized by a clear seasonality.

The Management Board believes the company is very well positioned to capitalize on future market opportunities. To this end, significant investments have been further advanced, including the approvals for the SINA Cloud and the TI Gateway, which represent important milestones. These developments form the basis for further expanding the product portfolio and customer base and achieving further growth.

Against this backdrop, the Management Board considers the results of financial year 2025 to be good. The renewed revenue growth, profitability, and strategic progress underscore the company's competitiveness and innovative strength. The focus remains on securing sustainable growth and further strengthening the company.

Business performance of secunet AG

secunet AG's management is based on the key performance indicators (KPIs) of revenue, EBITDA, and EBIT. The company's financial performance is directly dependent on the performance of the entire group. Accordingly, for financial year 2025, secunet AG was projected to achieve revenue of approximately €400 million, an EBIT margin between 11.5% and 13.5%, and an EBITDA margin between 14.5% and 16.5%.

In financial year 2025, secunet AG recorded revenues of €438.1 million (previous year: €389.3 million, forecast: approximately €400 million). At the same time, EBIT increased to €65.8 million (previous year: €51.1 million) and EBITDA to €69.7 million (previous year: €55.2 million). This resulted in an EBIT margin of 15.0% (forecast: 11.5–13.5%), while the EBITDA margin was 15.9% (forecast: 14.5–16.5%). Further details on these developments can be found in the section "Business Performance of the secunet Group".

The Management Board assesses the overall business performance of secunet AG in the 2025 financial year as good.

Results of operations

Results of operations of the Group

The statement of profit or loss for the secunet Group, prepared according to IFRS, as applicable in the EU, is prepared using the cost of sales method.

Incoming orders and order book

Incoming orders increased by approximately 26% to €531.9 million in financial year 2025 (previous year: €421.4 million). This is primarily attributable to the Public Sector segment, which saw significant growth, particularly in the fourth quarter. As a result, the order book as of December 31, 2025, also increased by approximately 36% to €278.9 million, exceeding the previous year's order book of €205.3 million. The order book mainly comprises orders from public sector clients as well as orders for financial year 2025 and subsequent years.

Sales revenue performance

In financial year 2025, the secunet Group recorded sales revenue of €458.8 million, representing an increase of 12.9% compared to the previous year (€406.4 million). Product sales, encompassing hardware, software, maintenance, and support, generated a total of €410.8 million in revenue in financial year 2025 (previous year: €353.5 million). Revenue from service billing declined to €48.0 million in 2025 (previous year: €52.8 million).

The secunet Group's business focus remained on federal ministries, national and international government institutions, and defense organizations. 89.8% of the Group's revenue in financial year 2025 was attributable to this target group (previous year: 91%). The Public Sector segment, which covers these activities, generated revenue of €412.2 million in the reporting period, representing an increase of 12% compared to the previous year (€369.7 million). As in previous years, the successful product business with the SINA product family was a key driver of revenue growth. Within this segment, the Defence & Space division, in particular, was able to increase its share of the overall annual success with high double-digit growth rates, contributing approximately one-third to the Group's revenue for the year. A similarly positive dynamic was also evident in the Homeland Security division, while the Public Authorities division was temporarily impacted by the prolonged delay in the federal budget. However, the division showed stronger growth again towards the end of the year.

The remaining 10.2% of Group revenue was attributable to the Business Sector segment (previous year: 9%). This segment serves two markets in the private sector: healthcare and industry. In financial year 2025, the Business Sector generated revenue of €46.6 million, also representing a significant increase compared to the previous year (€36.7 million).

The secunet Group recorded positive growth in both the German market and its international business in financial year 2025. In Germany, revenue increased by 11% from €366.3 million in the previous year to €408.1 million in the current reporting period. Internationally, secunet generated revenue of €50.7 million, compared to €40.1 million in the previous year, representing an increase of 27%. The share of international business in total revenue remained unchanged at approximately 11%.

The increase in Group sales revenue resulted from higher sales volumes and increased prices. Since the secunet Group operates primarily in the Eurozone, currency effects were negligible. Revenue from projects with the parent company Giesecke+Devrient remained at a low level of €0.5 million (previous year: €0.7 million).

Earnings performance

In financial year 2025, the secunet Group generated a gross profit of €106.3 million with a gross margin of 23.2% (previous year: 23.9%). This represents an improvement of €9.0 million, or 9.2%, compared to the previous year, primarily due to increased sales volume.

Cost of sales represents the most significant cost item in the secunet Group and comprises, as key components, material costs and personnel expenses. In the reporting year, cost of sales increased by 14.1% from €309.1 million in 2024 to €352.5 million, thus increasing at a similar rate to revenue growth.

The secunet Group's **selling expenses** rose to €30.1 million in 2025 (previous year: €28.8 million) due to further expansion of sales activities. The ratio of selling expenses to sales revenue decreased from 7.1% to the current 6.6%.

General **administrative expenses** amounted to €12.5 million. The increase of 8.2% compared to the previous year (€11.6 million) is attributable to higher

personnel and material costs in management and administrative departments. The ratio of administrative expenses to sales revenue decreased moderately from 2.9% in the previous year to 2.7% in the reporting period.

Research and development costs, i.e., expenditures related to in-house research and development for new products, totaled €11.4 million in 2025 (previous year: €13.7 million). These expenditures were incurred in connection with various projects, which are explained in more detail in the "Investments" section. The ratio of research and development costs to sales revenue was 2.5%, compared to 3.4% in the previous year.

Due to the developments described, the secunet Group generated **EBIT** of €51.6 million in the financial year. This corresponds to an EBIT margin of 11.3%. In the previous year, the secunet Group achieved EBIT of €42.5 million with a margin of 10.5%.

The Public Sector segment recorded an EBIT of €55.1 million in financial year 2025, compared to €44.8 million in the previous year. The Business Sector segment achieved an EBIT of -€3.4 million, compared to -€2.3 million in the previous year.

Interest income remained negligible in 2025 (€0.7 million, previous year: €0.8 million). Interest expenses amounted to €0.9 million, compared to €1.4 million in the previous year. The decrease is mainly attributable to the elimination of the interest accrual on the earn-out liability, which had increased interest expenses on a one-off basis in the previous year.

EBITDA increased by 24.2% to €74.9 million in financial year 2025 (previous year: €60.3 million). This increase is primarily attributable to a stable cost structure coupled with rising revenues. Depreciation rose to €23.2 million in the past financial year, compared to €17.8 million in the previous year. This increase is mainly due to an unscheduled write-down of the SysEleven brand in the past financial year.

In financial year 2025, the secunet Group achieved earnings before taxes **(EBT)** of €51.5 million, compared to €41.9 million in the previous year. The effective tax rate, based on the Group's earnings before taxes, was 35.2% in the reporting year (previous year: 33.4%).

As a result, the secunet Group recorded a **consolidated net income** of €33.3 million, compared to €27.9 million in the previous year. Of this, €33.3 million was attributable to the shareholders of secunet AG (previous year: €28.0 million), while non-controlling interests amounted to €0.0 million in 2025 (previous year: €0.0 million to minority shareholders of secustack GmbH). Diluted and basic earnings per share amounted to €5.15, compared to €4.32 in the previous year.

Results of operations of secunet AG

In the annual financial statements of secunet AG issued pursuant to the German Commercial Code (HGB), the profit and loss statement is presented using the nature of expense method.

In financial year 2025, secunet AG generated **sales revenue** of €438.1 million, compared to €389.3 million in the previous year and approximately €400 million in the forecast. The revenue increase is attributable to the same developments as within the Group. Other operating income amounted to €7.2 million, compared to €3.7 million in the previous year. This included public project grants, compensation payments, income from the reversal of provisions, and other income. Changes in inventories of work in progress and finished goods increased to €6.2 million in financial year 2025, compared to an increase of €1.6 million in the previous year due to pre-production and deliveries in 2026.

Material costs rose to €238.5 million due to increased sales volume, compared to €208.3 million in the previous year. **Personnel costs** increased to €101.3 million due to workforce growth and general wage adjustments, compared to €94.8 million in the previous year.

Depreciation of property, plant and equipment and amortization of intangible assets remained slightly below the previous year at €3.9 million in financial year 2025 (€4.1 million). This resulted primarily from the company's property, plant and equipment, with office equipment and IT infrastructure being the main components. Other operating expenses increased to €42.0 million compared to €36.3 million in the previous year. This increase resulted from various cost items, including office rent, advertising expenses, employee benefits, and vehicle expenses.

EBITDA at secunet AG increased by 26% from €55.2 million to €69.7 million. This is primarily due to increased sales volume combined with a stable cost structure.

secunet AG's **EBIT** for the 2025 financial year was significantly better at €65.8 million than in the previous year (€51.1 million).

The **financial result** for 2025 was -€23.2 million, primarily due to the initial absorption of losses under the profit and loss transfer agreement (EAV) with SysEleven GmbH, an extraordinary write-down of €17.4 million on the shares in SysEleven GmbH, and a reversal of a previous impairment loss on secunet International GmbH (formerly: finally safe GmbH). In the previous year, a profit of €0.6 million had been achieved.

Earnings before taxes **(EBT)** thus reached €42.7 million, compared to €51.7 million in the previous year.

After deducting income taxes of €18.5 million (previous year: €16.4 million) and other taxes of €0.0 million (previous year: €0.0 million), the **net income** decreased to €24.1 million compared to €35.3 million in the previous year.

Financial position and net assets

Financial position and net assets of the Group

The financial statements of the secunet Group are prepared in accordance with IFRS, as applicable in the EU.

Group capital structure

The secunet Group's total assets as of December 31, 2025, amounted to €410.7 million, representing an increase of 14.2% compared to December 31, 2024 (€359.6 million). On the asset side, this increase was primarily due to a rise in trade receivables and cash equivalents. On the liabilities side of the statement of financial position, equity amounted to €167.0 million (December 31, 2024: €150.8 million) and debt amounted to €243.7 million (December 31, 2024: €208.8 million). The equity ratio decreased slightly to 40.7% as of December 31, 2025 (previous year: 41.9%), while the debt ratio increased slightly to 59.3% (previous year: 58.1%).

As of the reporting date, short-term loans and the current portion of long-term loans amounted to €1.5 million, compared to €1.3 million on December 31, 2024. Financing of ongoing business operations and necessary replacement investments during the reporting period was primarily derived from operating cash flow.

Statement of financial position of the secunet Group, assets

in euros	31.12.2025	31.12.2024
Current assets		
Cash and cash equivalents	87,407,578.85	57,682,113.94
Trade receivables	102,902,430.22	84,807,157.94
Financial assets from affiliated companies	215,247.99	42,680.84
Contract asset	4,922,901.53	3,286,668.57
Inventories	64,236,317.74	53,852,840.96
Other current assets	6,041,837.30	6,742,352.92
Income tax receivables	1,514,297.32	1,337,152.14
Current assets, total	**267,240,610.95**	**207,750,967.31**
Non-current assets		
Property, plant and equipment	13,307,930.67	13,353,481.00
Right-of-use assets	18,206,632.34	22,263,140.52
Intangible assets	28,517,107.54	36,694,810.65
Goodwill	47,627,601.69	47,627,601.69
Non-current financial assets	6,432,376.30	6,306,820.30
Deferred taxes	3,496,716.93	5,852,002.00
Other non-current assets	25,891,252.22	19,800,609.62
Total non-current assets	**143,479,617.69**	**151,898,465.78**
Total assets	**410,720,228.64**	**359,649,433.09**

Assets

The asset side of the consolidated statement of financial position showed current assets of €267.2 million as of December 31, 2025, representing an increase of 28.6% compared to €207.8 million on the previous year's date.

Cash and cash equivalents increased to €87.4 million due to cash inflows from operating activities, compared to €57.7 million at the same time of the previous year. This was offset by investments in intangible assets and property, plant and equipment, as well as dividend payments.

Due to revenue growth, **receivables from deliveries and services** increased from €84.8 million on December 31, 2024 to €102.9 million as of the current reporting date.

At the end of the year, **inventories** of €64.2 million were carried forward to the new financial year (December 31, 2024: €53.9 million). This increase is primarily due to the generally higher sales level.

The **contract assets** as of December 31, 2025, amounted to €4.9 million, compared to €3.3 million on the same date of the previous year. These values represent services already rendered under contracts for work or services, for which no unconditional claim for payment has yet arisen.

Receivables from income taxes amounted to €1.5 million at the reporting date, compared to €1.3 million at the same date of the previous year. This increase was primarily due to higher advance tax payments during the financial year.

Non-current assets totaled €143.5 million as of December 31, 2025, a decrease compared to the previous year (€151.9 million).

Goodwill remained unchanged from the previous year at €47.6 million. **Intangible assets** decreased to €28.5 million in the financial year, compared to €36.7 million at the same time of the previous year. This is primarily due to the extraordinary write-down of the SysEleven brand. **Property, plant, and equipment**, consisting mainly of office equipment and IT infrastructure, declined slightly to €13.3 million, compared to €13.4 million in the previous year.

Rights-of-use amounting to €18.2 million (December 31, 2024: €22.3 million) decreased compared to the previous year, primarily due to a lower number of new lease agreements for buildings, offices, and company cars relative to lease payments. The corresponding item on the liabilities side is lease liabilities.

Current and non-current other assets increased to €31.9 million (as of December 31, 2024: €26.5 million). These consist mainly of other receivables from suppliers, advance payments for travel expenses, prepayments for future services, and other receivables.

Debt and equity

On the liabilities side, **current liabilities** rose to €140.6 million as of December 31, 2025, compared to €115.8 million in the previous year, while **non-current liabilities** increased from €93.0 million to €103.1 million. As of the reporting date, short-term loans and the current portion of long-term loans amounted to €1.5 million, remaining essentially stable compared to the previous year's reporting date (€1.3 million).

Statement of financial position of the secunet Group, liabilities

in euros	31.12.2025	31.12.2024
Current liabilities		
Trade payables	52,955,061.07	41,611,809.36
Liabilities to affiliated companies	274,261.41	151,549.96
Lease liabilities	6,365,206.37	6,299,664.89
Short-term loans and current portion of long-term loans	1,473,842.74	1,289,258.41
Other provisions	28,903,925.24	25,331,506.94
Income tax liabilities	3,257,434.22	760,642.62
Other current liabilities	12,175,084.63	7,274,804.30
Contract liabilities	35,145,615.02	33,124,992.52
Total current liabilities	**140,550,430.70**	**115,844,229.00**

Statement of financial position of the secunet Group, liabilities

in euros	31.12.2025	31.12.2024
Non-current liabilities		
Lease liabilities	12,350,057.83	16,576,462.14
Other non-current liabilities	2,084,359.10	2,870,595.94
Deferred taxes	8,669,411.62	11,229,546.92
Pension provisions	5,696,664.00	6,360,121.00
Other provisions	4,641,597.73	2,708,865.09
Contract liabilities	69,694,880.71	53,226,350.08
Total non-current liabilities	**103,136,970.99**	**92,971,941.17**
Equity		
Subscribed capital	6,500,000.00	6,500,000.00
Capital reserves	21,922,005.80	21,922,005.80
Other reserves	217,984.89	-383,196.11
Retained earnings	138,392,836.26	122,710,681.16
Equity attributable to the shareholders of the parent company	**167,032,826.95**	**150,749,490.85**
Non-controlling interests	0.00	83,772.07
Total equity	**167,032,826.95**	**150,833,262.92**
Total liabilities	**410,720,228.64**	**359,649,433.09**

Against the backdrop of continued growth in sales revenue, **trade payables** also increased by 27.3% as of the reporting date. They reached €53.0 million on December 31, 2025, compared to €41.6 million in the previous year.

Lease liabilities amounted to €18.7 million as of the reporting date, compared to €22.9 million in the previous year. These liabilities resulted primarily from lease agreements for buildings, offices, and company cars. On the asset side, these liabilities are offset by the corresponding right-of-use assets.

Contract liabilities increased to €104.8 million as of December 31, 2025 (December 31, 2024: €86.4 million) and included customer advance payments that will be recognized as revenue after the reporting date. This item records transactions in which secunet generates advance payments or receives down payments for future deliveries or services due to multi-year maintenance and support contracts and extended warranties. The increase is primarily attributable to growth in the product business.

Due to increasing drawdowns from pension payments, there was a slight reduction in pension provisions. As of December 31, 2025, they amounted to €5.7 million, compared to €6.4 million on the previous year's date.

Other provisions increased to €28.9 million as of the reporting date (December 31, 2024: €25.3 million). This increase resulted primarily from the creation of provisions for variable compensation components of the workforce.

Other **current liabilities** increased to €12.2 million as of the reporting date, compared to €7.3 million in the previous year. Other long-term liabilities, on the other hand, remained virtually unchanged at €2.1 million in the financial year, compared to €2.9 million at the same date in the previous year.

Deferred tax liabilities decreased to €8.7 million compared to €11.2 million in the previous year. These liabilities primarily included deferred tax liabilities arising from intangible assets in connection with the acquisition of SysEleven GmbH in 2022.

The **equity** of the secunet Group increased from €150.8 million as of the 2024 reporting date to €167.0 million as of December 31, 2025. This is primarily due to the increase in retained earnings, which rose from €122.7 million to €138.4 million. However, relative to total assets, the equity ratio decreased slightly to 40.7% (December 31, 2024: 41.9%), mainly attributable to the increase in liquid assets.

Cash flow and liquidity

In financial year 2025, the secunet Group recorded a **cash flow from operating activities** of €62.5 million. This represents a slight increase compared to the previous year (€61.0 million), but less than the overall increase in profitability. This is primarily attributable to higher tax payments resulting from the improved consolidated net income.

Cash flow from investing activities amounted to -€8.2 million in the reporting period, significantly below the prior year's figure (-€22.7 million). This decline is primarily attributable to the absence of the earn-out component of -€8.8 million due in 2024 from the acquisition of SysEleven GmbH. At the same time, investments in capitalizable software decreased noticeably.

The **cash flow from financing activities** of -€24.5 million (previous year: -€21.8 million) essentially reflects the dividend payment of €17.7 million (previous year: €15.3 million) and repayments of lease liabilities of €7.0 million (previous year: €6.6 million).

Following the close of the 2025 financial year, **total cash and cash equivalents** amounted to €29.7 million, compared to €16.4 million in the previous year. Cash and cash equivalents totaled €87.4 million as of December 31, 2025, significantly exceeding the figure for the previous year (€57.7 million). To ensure additional financial flexibility, secunet has a credit facility of €30 million.

Financial position and net assets of secunet AG

The financial statements of secunet AG were prepared in accordance with German commercial law. The accounting treatment in the financial statements of secunet AG differs from that of the secunet Group (prepared in accordance with IFRS), as applicable in the EU, primarily in the accounting for fixed assets, receivables, inventories, pension provisions, and deferred taxes.

Goodwill is also accounted for differently. Under the German Commercial Code (HGB) it is amortized on a straight-line basis, whereas under IFRS it is not amortized but tested for impairment.

Balance sheet secunet AG, assets

in euros	31.12.2025	31.12.2024
A. Fixed assets		
I. Intangible assets	661,736.00	923,505.00
II. Property, plant and equipment	7,569,783.00	7,501,278.00
III. Financial assets	76,209,700.84	89,040,595.04
Total fixed assets	84,441,219.84	97,465,378.04
B. Current assets		
I. Inventories	62,625,545.66	55,579,671.50
II. Receivables and other assets	106,378,441.98	86,404,294.70
III. Cash on hand and balances with credit institutions	82,879,356.04	53,819,380.22
Total current assets	251,883,343.68	195,803,346.42
C. Prepaid expenses and accrued income	30,099,118.43	24,059,251.15
Total assets	**366,423,681.95**	**317,327,975.61**

The **total assets** of secunet AG increased to €366.4 million as of December 31, 2025, compared to €317.3 million as of December 31, 2024. On the asset side of the balance sheet, **fixed assets** decreased from €97.5 million in the previous year to €84.4 million as of December 31, 2025. **Financial assets** amounted to €76.2 million (December 31, 2024: €89.0 million) and comprised shares in affiliated companies and investments. **Property, plant, and equipment** amounted to €7.6 million (previous year: €7.5 million). Due to scheduled amortization, **intangible assets** decreased to €0.7 million (December 31, 2024: €0.9 million).

Current assets increased to €251.9 million as of December 31, 2025, representing a rise of 28.6% compared to the previous year (€195.8 million). This increase resulted primarily from the rise in **cash and cash equivalents** to €82.9 million due to cash inflows from operating activities (December 31, 2024: €53.8 million). **Receivables and other assets** rose to €106.4 million (December 31, 2024: €86.4 million). A key reason for this is the increased sales volume. At the same time, inventories increased from €55.6 million in the previous year to €62.6 million as of December 31, 2025. The reasons for these developments largely correspond to those within the Group.

Prepaid expenses and accrued income amounted to €30.1 million (December 31, 2024: €24.1 million), mainly due to advance payments for product services sold as part of customer projects.

Balance sheet secunet AG, liabilities

in euros	31.12.2025	31.12.2024
A. Equity		
Subscribed capital	6,500,000.00	6,500,000.00
Nominal value of treasury shares	-30,498.00	-30,498.00
I. Issued capital	6,469,502.00	6,469,502.00
II. Capital reserves	21,656,305.42	21,656,305.42
III. Retained earnings		
Other retained earnings	116,662,774.13	109,250,451.13
IV. Net accumulated profit	16,691,315.16	17,661,740.46
Total equity	161,479,896.71	155,037,999.01
B. Provisions	46,064,797.25	37,293,050.28
C. Liabilities	63,498,152.20	47,046,902.25
D. Deferred income and accrued expenses	95,380,835.79	77,950,024.07
Total liabilities	**366,423,681.95**	**317,327,975.61**

As of December 31, 2025, secunet AG's equity amounted to €161.5 million, compared to €155.0 million in the previous year.

Provisions amounted to €46.1 million as of the reporting date (€37.3 million as of December 31, 2024) and mainly comprised provisions for pensions and similar obligations, tax provisions and other provisions.

Liabilities increased by approximately 35% to €63.5 million as of December 31, 2025, compared to €47.0 million on the same date of the previous year. This increase is primarily attributable to higher material purchases in the fourth quarter to handle the increased order volume.

Deferred income and accrued expenses increased to €95.4 million at the reporting date, compared to €78.0 million at the same date of the previous year. This is attributable to the growing product business, which resulted in increased revenue being deferred in connection with services rendered after the reporting date.

Proposal for the appropriation of profits

The Management Board and Supervisory Board will propose at the Annual General Meeting to be held on June 8, 2026, that an amount of €16.7 million be distributed to the shareholders as a dividend of €2.58 per share on the 6,469,502 shares of the share capital as of December 31, 2025, from the net income of €16.7 million for financial year 2025 of secunet AG.

Investments

In financial year 2025, the secunet Group invested €8.2 million in intangible assets and property, plant, and equipment. This primarily involved expenditures for the acquisition and replacement of hardware, software, and other operating equipment, as well as investments in internally developed software. In the previous year, €14.1 million was spent on these items.

During the same period, secunet AG invested €3.8 million, compared to €4.6 million in the previous year. The majority of these funds were used to replace hardware and other operating and business equipment.

Employees

As of December 31, 2025, the secunet Group employed 1,171 permanent staff. Compared to the previous year (1,059 permanent staff), the number of employees increased by 112, or 11%. In addition, the secunet Group employed 106 temporary staff as of the same date (December 31, 2024: 123 temporary staff). In total, 1,277 people were employed by the secunet Group (December 31, 2024: 1,185). The increase in the number of employees is solely attributable to organic growth.

At the end of the 2025 financial year, secunet AG employed 964 permanent staff (December 31, 2024: 869).

Overall statement on the results of operations, financial position and net assets

The Management Board continues to assess the economic situation of the Group and the Company as good at the time of reporting.

The increase in sales revenue shows that the secunet Group can continue to achieve significant growth. Furthermore, the company has successfully expanded and diversified its product portfolio. EBIT also increased compared to the previous year. The Management Board is convinced that these investments represent an essential step required for the company's medium- and long-term growth and will unlock additional growth potential.

The positive results and cash-generating business model of the secunet Group have led to a healthy cash flow from operating activities. This financial strength is also reflected in a strong statement of financial position, particularly in a more than solid equity ratio of 40.7%.

Risk and opportunity report

Objectives and methods of risk and opportunity management

Risk and opportunity management (hereinafter referred to as ROM) is carried out in the same way and in parallel for the secunet Group and for secunet AG. Therefore, the functions described below, as well as the descriptions of individual risks and opportunities, apply to both the secunet Group and secunet AG.

At secunet, ROM takes place on multiple levels. Accordingly, the assessment of the risk and opportunity situation draws on various sources.

Risks and opportunities with regard to the objectives set out in the current annual plan are addressed in a dedicated risk committee, the ROM Committee.

Recurring operational risks and opportunities are taken into account within the framework of regular operational routines and risk minimization or opportunity maximization measures and are largely reduced or eliminated (risks) or supported (opportunities).

Risks and opportunities, which are addressed through strategic, medium- to long-term measures, are taken into account by the Management Board as framework conditions for medium-term strategic corporate planning.

secunet AG's early risk detection and risk and opportunity management systems are continuously being developed and optimized.

Risk and opportunity management for the current planning and financial year

Risk and opportunity management (ROM) with regard to the objectives set out in the current annual plan is carried out at secunet by a risk committee, the ROM Committee. This committee comprises the members of the Management Board and the head of the risk management department. The ROM Committee meets regularly once a quarter as part of an Management Board meeting. Developments that could pose a threat to achieving the objectives or even to the continued existence of the company are presented in a risk report and discussed by the ROM Committee. The aim is to obtain information about risks and their associated financial impacts as early as possible in order to take appropriate measures. At the same time, existing opportunities and their associated earnings potential should also be identified and utilized.

In preparation for the ROM Committee meetings, a comprehensive risk and opportunity inventory is conducted across all areas of the company. Using a bottom-up approach, the material risks and opportunities are identified, assessed according to their potential impact or contribution to success, and aggregated based on their probability of occurrence. The aim is to capture material risks and opportunities, for which a materiality threshold of 1% or more from the respective planned figure has been established. In principle, all risks can be included; however, inclusion is mandatory for risks exceeding the materiality threshold. Parallel to the risk and opportunity inventory, this data is validated by comparing it with the ongoing sales and profit forecasts maintained by the Sales Management and Controlling departments. The results of this validation are also incorporated into the risk and opportunity inventory.

Since February 28, 2026, there has been an armed conflict between the United States of America (USA) and the State of Israel on one side, and the Islamic Republic of Iran (Iran) on the other. We have discussed and reviewed potential impacts on the secunet Group. At the time this report was prepared (mid-March 2026), no specific, material risks requiring separate assessment could be identified. However, due to the very short time period under consideration, a definitive assessment is not possible.

The company-specific risks and opportunities identified in this way are discussed top-down in the meetings of the ROM Committee and revalidated as needed. When considering the potential damaging effects of risks and the positive impact of opportunities, a net approach is used, meaning that the effects of previously implemented risk mitigation and opportunity improvement measures are factored into the assessment. Depending on the probability-weighted damage value of the risks and the positive impact of the opportunities (risk value and opportunity value), the further handling of the risks and opportunities is determined according to uniform principles of action. These range from mere documentation in cases of negligible value (in financial year 2025, the probability-weighted loss/opportunity value for the secunet Group is less than approximately €0.8 million for the EBIT loss, "low risk/low opportunity") to further monitoring and tracking of existing measures (in financial year 2025, the loss/opportunity value for the secunet Group is less than approximately €2.8 million, "medium risk/medium opportunity") to the necessity of taking and tracking immediate action (reporting threshold – in financial year 2025, the probability-weighted loss/opportunity value for the secunet Group is above approximately €2.8 million, "high risk/high opportunity").

The defined threshold values are redefined annually based on the projected annual results. If the identified risks/opportunities are quantifiable, the corresponding (date-specific) risk/opportunity values are included in the reporting.

Subsequently, if necessary, proposals for countermeasures to risks and support measures to address opportunities are developed. The Management Board reviews these measures and ensures their timely implementation.

The operational risks and opportunities considered in this part of the ROM for the secunet Group, and thus also for secunet AG as the parent company, are mainly categorized according to their origin in the functional areas of secunet into

- Sales risks/sales opportunities: These are risks and opportunities in all areas related to distribution. They primarily concern the functions of purchasing and inbound logistics, sales and outbound logistics, as well as sales and marketing.

- Product risks/product opportunities: These are the risks and opportunities that can arise in connection with secunet's products and solutions. They primarily concern risks stemming from technical defects or potential safety weaknesses in the components used. In addition, there are risks from the areas responsible for planning and coordinating the market readiness of secunet Group products and solutions.

- Project risks/opportunities: These are the risks and opportunities that can arise in connection with development and consulting projects. These primarily include the risks of budget planning and subsequent adherence to the budget. Opportunities can arise if projects are completed better than planned.

- Structural risks/opportunities: These are the risks and opportunities arising from support functions such as finance and controlling, legal and human resources, and IT. Risks from M&A activities and compliance risks are also included here.

At the time of preparation of this report, the risk and opportunity situation with regard to operational risks is as follows:

- Sales risks primarily include risks arising from the postponement of major projects, for example, due to budget cuts by major clients. These sales risks are offset by sales opportunities arising, for instance, from large new projects or the expansion of existing major public sector projects. Risks from supply bottlenecks also fall under the category of sales risks. These are mitigated through active supply chain management (for example, by building up inventory and maintaining close, ongoing coordination with key suppliers).

- Product risks primarily arise from longer than expected time expenditure for the development and approval of new products. This indirectly affects the sales opportunities for these products.

- The project risks consist primarily of budget deviations. These are mitigated through coordination with the clients (budget adjustments, change requests in the project plans) and by including the risks in the forecast (profit adjustments).

- Structural risks – such as impending write-downs on inventories or other unplanned expenses – are more than compensated for by opportunities in this category.

Operational risk and opportunity management

Operational risks and opportunities are risks/opportunities inherent in ongoing business operations that can recur. They are identified, assessed, and, where possible, eliminated or exploited through specific risk minimization and opportunity enhancement routines. These control mechanisms are implemented at various points in the value creation process and are documented in the Internal Control System (ICS).

Sales and distribution risks are discussed within the framework of sales coordination via risk committees. Risk committee meetings are mandatory for orders exceeding a certain threshold. These committees consist of at least representatives from the responsible (sales) department, the division/business unit likely to be awarded the contract, the commercial director, representatives from the legal and purchasing departments, and a member of the Management Board. The objective of the risk committees is to decide, based on transparent criteria, whether and how to submit a bid or accept a contract for the respective order or tender. A standardized, synoptic presentation of the risks and opportunities associated with the respective tender serves this purpose.

Since the risk committees each discuss the risks, including an assessment of their acceptability, and the decisions acknowledge the risks as acceptable, they are considered low at the time of this report.

Large-scale projects inherently carry project management risks. In addition, long-term large-scale projects present specific risks. At secunet, these project risks are identified, assessed, and mitigated through appropriate measures within the overarching project coordination process. Project management risks arise after the commissioning of large-scale projects: their sheer scale inherently introduces numerous uncertainties during implementation. These risks include, for example, failure to adhere to schedules and project budgets. secunet addresses these risks through comprehensive project management, which generates regular control reports for project management, business unit management, and the Management Board. Risks arising from large-scale projects—like development risks—are continuously monitored through comprehensive project planning and control mechanisms, combined with risk-oriented reporting. In the event of deviations from the established targets, risk mitigation measures are immediately decided upon and implemented. These measures may include providing additional resources for project work and discussing deviations with clients to align their expectations with the changed circumstances. The risks arising within the scope of project management are adequately mitigated through appropriate measures. Accordingly, the project risks mentioned are considered low at the time of writing this report.

No significant project risks existed at the end of 2025; accordingly, this risk class was classified as low.

Product risks can arise in various forms. These are largely mitigated through operational management processes, so they are considered low at the time of writing.

Product risks can arise in the various phases of the product lifecycle. During the development of new products – which also includes large-scale projects – the following risks are regularly discussed and assessed:

- The risk of potentially weak demand: The product does not prove successful in the market.
- The risk of technical malfunctions: The product has defects that lead to warranty claims.
- The risk of the product not being completed on time: The development project needs significantly more time than estimated.

Market risk and the risk of technical malfunctions do not exist at the time of this report's preparation. Only the latter development risks are considered. These primarily impact sales risk within the risk assessment for the current financial year.

In the past, secunet developed products and solutions primarily as a result of contracts to meet specific security needs in the public sector. IT high security was strongly customer-oriented; products were generally not designed without specific requirements. Most secunet developments were contract-driven and accordingly financed by the commissioning customers. Therefore, development risks related to potential lack of demand were not a concern. Consequently, risks arising from the development of new products that ultimately failed to gain market acceptance were of minor importance to secunet in most product areas.

The development of secunet's own products, such as the secunet connector, the SINA Communicator, and the easykiosk, has increased the volume of associated internal investments in recent years. This has brought development risks more sharply into focus for risk assessment. The focus here is less on the sales prospects associated with the products and more on the duration of development and approval. The greatest risk in development projects can lie in underestimating the time required to reach acceptance readiness. This can lead to time and personnel expenditures that limit the project's profitability. To minimize these risks, secunet employs comprehensive project planning and control mechanisms at various stages, combined with a dedicated reporting line. This aspect of risk analysis and risk management aligns with the activities related to large-scale projects. For development projects, the risk is currently classified as low.

The product portfolio of secunet AG focuses on cybersecurity solutions, specifically the SINA product family, which comprises cryptographically secured and certified solutions of a high standard. One risk continuously assessed in connection with the technical characteristics of these products is the impact of potential – as yet undiscovered – security vulnerabilities. This involves investigating whether and to what extent security gaps in individual components compromise secunet's security promise to its customers. This is the task of operational incident management, another component of secunet's risk management. To minimize risk, a comprehensive process of continuous risk identification and assessment is in place. As part of this process, secunet gathers and evaluates information from a wide variety of sources regarding potential security risks. If this assessment reveals even the slightest possibility of vulnerability to the systems, customers are immediately notified and supported in closing the potential security gap. This process of monitoring and resolving potential technical security risks is implemented in close coordination with the development and approval partner, the Federal Office for Information Security (BSI). Given the implemented risk minimization measures, the economic risk associated with technical product security is considered low.

Strategic risk and opportunity management

Medium- and long-term risks and opportunities for secunet are considered within the framework of strategic planning. These are grouped into the risk and opportunity categories of strategic risks (e.g., macroeconomic conditions, market dynamics and developments in the competitive landscape, as well as risks associated with investments, M&A activities, and capital market risks) and risks related to sustainability and compliance. A discussion of these framework conditions and their consequences for the strategy takes place regularly as part of the planning process and with the Supervisory Board, which approves and monitors this plan.

The risks considered here include, but are not limited to, the following:

Macroeconomic developments such as the economic cycle (potential recession), inflation, and interest rate trends are considered, but are not deemed significant for secunet. This is because secunet's products have primarily been involved in public infrastructure projects, which are considerably less susceptible to economic fluctuations than private sector projects. Inflation expectations are factored into the planning. Furthermore, secunet has only taken out short-term loans and is therefore relatively independent of interest rate developments.

Market risks are more than offset by market opportunities. Risks include rapid technological change, which creates intense pressure to innovate, and increasing competitive pressure resulting from the attractiveness of the IT security market. Opportunities arise from the fundamental market growth

driven by increasing digitalization, complemented by the desire for digital sovereignty and cyber resilience. Trustworthy IT security products made in Germany are therefore in high demand. Regulatory requirements, such as those arising from the IT Security Act, further fuel this demand.

Potential risks include secunet's focus on the German market and its target group of public sector clients with a relatively small number of large customers, who are essentially served by a single product family (SINA). While these aspects can also be interpreted as a stable foundation for a sustainable business, secunet's strategy also envisions leveraging growth opportunities in the private sector and international markets.

As in operations, supply risks are considered highly significant in the strategy. Geopolitical developments ("America First" orders, the war in Ukraine, the war in the Middle East, changes in procurement relationships) exacerbate the already strained supply situation on the international semiconductor market. This is particularly acute for secunet because often only a few suppliers are authorized for high-security applications. This single-source dependency makes it virtually impossible to switch to alternative suppliers. Therefore, consistently risk-minimizing supply chain management is crucial both operationally and strategically. Past operational experience has demonstrated secunet's ability to manage these challenges and gives reason for optimism regarding the medium-term future.

On the recruitment side, the shortage of skilled workers and demographic trends pose challenges for the future. secunet is therefore committed to maintaining its reputation as an attractive employer.

Acquisitions continue to be seen as a strategic opportunity for growth. The acquisition of SysEleven GmbH in financial year 2022 demonstrated secunet's ability to execute successful transactions. secunet remains actively engaged in identifying suitable and economically viable acquisition targets.

Overview of risks and opportunities

A comprehensive review of the risks and opportunities that could influence the further development of the secunet Group leads to an overall positive assessment. The assessment has shown that, at the time of preparation of this report, the risks are generally manageable and that the identified risks do not pose any threat to the continued existence of the Group and the Company with regard to illiquidity or over-indebtedness during the reporting period of at least one year. The overall risk position has not changed significantly compared to the previous year. The identified opportunities support this assessment. The Group's operational management consistently implements measures to prevent an increase in the risk position. At the same time, numerous activities are being undertaken to promote the exploitation of the described opportunities. As of the reporting date, no significant risks exist.

The business development of secunet AG is subject to the same risks and opportunities as that of the Group. Therefore, the presentation and assessment of risks and opportunities apply equally to secunet AG.

Forecast

Premises of the forecast

The forecasts for the secunet Group and secunet AG include all information known to the Management Board at the time of preparation of this report that could have an impact on business performance. The outlook is based, among other things, on the expectations described below regarding economic developments and the development of the IT and IT security market.

With regard to the secunet Group and its individual segments, Public Sector and Business Sector, unforeseen events could influence the development of the company or individual business units that is expected from today's perspective.

The projected developments in the financial performance indicators relate exclusively to the development of the secunet Group within the group structure as of the reporting date of December 31, 2025 (scope of consolidation).

Macroeconomic environment

For 2026, the German economy is projected to experience a moderate economic recovery, marking a cautious turnaround after years of stagnation and recession. The German government's current projection anticipates a 1.0% increase in gross domestic product (GDP). While more optimistic voices, such as the DIW Berlin, consider growth of up to 1.3% possible, the ifo Institute remains more reserved with a forecast of 0.8%. At the same time, global trade, due to geopolitical tensions and the threat of trade conflicts (e.g., with the USA), offers little support for Germany's export-oriented industry. The expected investment climate presents a mixed picture, with government investment expected to increase over the course of the year, while private companies remain hesitant.

Due to its high sales share, Germany represents the most important sales market for the secunet Group and secunet AG.

Sector-specific conditions

Information and communication technology (ICT) market

Besides the general economic development in Germany, the overall market for information technology and telecommunications (ICT) forms an essential framework for secunet. Market statistics are primarily compiled by the digital association Bitkom.

The German market for information and communication technology (ICT) is projected to grow by 4.4% to a volume of €245.1 billion in 2026. This growth will be driven primarily by information technology (IT), which is expected to see a revenue increase of 5.8% to €170.0 billion. Within IT, the software sector is expected to experience the strongest growth, with a projected increase of 10.2% to €58.3 billion, followed by IT hardware, which is expected to grow by 3.9% to €57.4 billion.

IT security market

According to current forecasts from Bitkom, spending on hardware, software, and services in the IT security sector will rise significantly again, reaching approximately €12.2 billion in 2026. This represents an increase of around 10% compared to the previous year.

The largest share of these expenditures is for services related to IT security, followed by investments in security software and hardware.

Increasing digitalization and the associated cyber threats are driving this growth. Companies are increasingly recognizing the need to invest in robust security solutions to protect themselves against increasingly sophisticated attacks.

Company-specific conditions

Strategy

secunet pursues a clear strategy based on sustainable and profitable growth in core markets, while also including targeted investments in promising growth areas. The primary focus is on strengthening its market position, seizing future opportunities, and creating value for all stakeholders.

secunet's strategy is consistently aligned with the changing geopolitical landscape and the associated massive increase in hybrid threats. In light of a tense IT security environment and increasingly aggressive, often state-sponsored cyberattacks, the company relies on a proactive defense architecture. This strategy aims to substantially strengthen the defense capabilities of Germany and Europe through highly secure, post-quantum-resistant cryptographic solutions and the protection of critical infrastructures (KRITIS).

A key pillar of the company's strategy is, among other things, the promotion of European data sovereignty. secunet counters the dominance of non-European providers with sovereign cloud ecosystems and on-premises AI solutions that ensure sensitive data is subject exclusively to European jurisdiction and protected from access by laws such as the US CLOUD Act. By integrating AI into cyber defense – for example, for the automated, real-time detection of anomalies – the company is transforming security from a purely reactive protective measure into a strategic competitive advantage.

Another key growth area lies in the defense sector. secunet has recently experienced significant growth in this area, driven by rising military spending and the need to protect armed forces against cyberattacks and sabotage. Through "Security made in Germany", secunet aims to create technological independence that empowers both government institutions and industry to achieve "sovereign digitalization" and enhances national resilience against global systemic risks.

In addition to these areas, secunet is focusing on expanding its business, with a particular emphasis on the healthcare sector and critical infrastructure. At the same time, its international presence is being strategically expanded.

Market position

The Management Board is of the opinion that secunet's products and solutions enjoy an excellent reputation. The company sees itself as a recognized provider of high-quality and trustworthy IT security for the most demanding requirements in the market. The IT security partnership with the Federal Republic of Germany, which has been in place since 2004, underscores this assessment. This positions the secunet Group exceptionally well to meet the increasing demand resulting from market growth.

IT security solutions "Made in Germany" enjoy an excellent reputation worldwide due to their quality and trustworthiness. International demand for high-quality solutions like those offered by secunet is increasing. In addition to the German market, secunet focuses on countries of the European Union, EU organizations, defense and space agencies (including organizations like NATO), and countries in the Middle East. The Management Board believes the secunet Group is ideally positioned to leverage the growth potential in international markets.

Acquisitions

The secunet Group aims for sustainable and profitable organic growth, which can be strategically supplemented by value-enhancing acquisitions. This could involve filling gaps in the portfolio and further strengthening technological expertise. Thanks to a stable balance sheet structure, the secunet Group has the financial resources to enable a continued development through organic growth, targeted acquisitions, and collaborations and partnerships.

Forecast for the secunet Group

Given the aforementioned conditions, the Management Board anticipates continued strong demand for the products and solutions of the secunet Group. This positive assessment is confirmed by the order book of €278.9 million at the end of financial year 2025.

The risks presented in the risk and opportunity report are considered manageable by the Management Board. In the Management Board's view, the opportunities outweigh the risks. Against this background, the Management Board assesses the anticipated development of the secunet Group positively.

For financial year 2026, the Management Board therefore anticipates further growth in both sales revenue and earnings. The key market drivers remain intact, as evidenced by the dynamic incoming orders in the past financial year.

Accordingly, the Management Board anticipates an increase in consolidated revenue to between €460 and €500 million for the 2026 financial year. A similarly positive trend is expected for operating profit, with EBIT projected at €53 to €58 million by year-end, while EBITDA is expected to rise to between €76 and €84 million.

Forecast for secunet AG

secunet AG is managed based on sales revenue, EBITDA, and EBIT. The Company's future economic performance is directly dependent on the performance of the Group as a whole. Accordingly, the statements in the forecast report for the Group apply equally to the company.

For the 2026 financial year, the Management Board of secunet AG therefore expects sales revenue of between €440 million and €480 million (2025: €438 million). This positive development will also have an impact on operating profit. Accordingly, EBITDA is expected to be between €76 million and €84 million, while EBIT is projected to be between €67 million and €72 million.

Risk reporting in relation to financial management

The financial management of the Company and the Group is fundamentally based on the provisions and requirements of corporate law. This ensures that all group companies can operate under the going concern assumption.

The secunet Group and its companies have always been able to meet their payment obligations. Liquid assets are invested with strict risk minimization. Ongoing monitoring of liquid assets and their alignment with liquidity requirements serve to ensure long-term solvency. This is also the primary objective of financial management.

As of the reporting date of December 31, 2025, a credit line totaling €45 million existed with various credit institutions. This served to proactively hedge the Group's liquidity.

Risk management and internal control system

secunet Security Networks AG and the secunet Group have an internal control system (hereinafter referred to as ICS) which pursues the following three objectives:

- Reporting: ensuring the accuracy and reliability of internal and external financial and non-financial reporting.
- Efficiency: ensuring the effectiveness and efficiency of business processes
- Compliance: supporting adherence to laws, regulations, contracts, and internal guidelines.

The ICS can be described using the following functions:

- Control environment and objectives of the ICS,
- Internal control system (ICS) process including risk assessment, control activities and reporting,
- Information and communication,
- Monitoring and improvement.

The internal control system (ICS) encompasses the principles, procedures, and measures for ensuring the effectiveness and efficiency of business operations, the regularity and reliability of internal and external financial reporting, and compliance with the legal regulations applicable to the company. It also serves to detect risks arising from potential legal violations and/or those that jeopardize company assets or objectives. Furthermore, it is an information system that supports the Management Board and all stakeholders in fulfilling their responsibilities.

The internal control system (ICS) is integrated into the secunet Group's corporate governance system. In addition to the ICS, which focuses primarily on managing process risks, the secunet Group maintains the following corporate governance systems: a risk management system, a compliance management system, and an internal audit system. These systems operate largely in parallel with the ICS. The necessary integration is achieved through the respective system owners, including information exchange in regular meetings and at the level of the responsible members of the Management Board.

All relevant (essential) processes and functions are included in the internal control system (ICS). Roles and responsibilities are clearly defined within the ICS.

The internal control system (ICS) process is designed as a cycle:

- New process creation including description of processes, risks and controls,
- Implementation and execution of control activities in the operational process,
- Regular effectiveness assessment and reporting,
- Control self-assessment: This involves comparing the currently valid processes and process risks with the current state of documentation in the internal control system (ICS). This determines whether the documented ICS corresponds to operational reality and whether the defined controls adequately cover the process risks. If not, the process owner must define additional controls or adjust the existing controls accordingly. The assessment of adequacy and effectiveness carried out in this way is supported and documented by Internal Audit.
- Implementation of potential improvements from the effectiveness assessment and the control self-assessment into control activities.

The internal control system (ICS) process is moderated by the ICS coordinator appointed by the Management Board. An IT solution is used for documenting the ICS, control confirmations, and self-assessments. Those responsible for the ICS process are trained in its use by the ICS coordinator.

Statement on the appropriateness and effectiveness of the governance systems[1]

In accordance with principles 4 and 5 of the German Corporate Governance Code (DCGK 2022), responsible management of the risks of business activities requires appropriate and effective governance systems (internal control system, risk management system and compliance management system) within the company.

As part of its ongoing internal control and monitoring activities, the Management Board regularly received and discussed reports on the governance systems during financial year 2025. These regular processes, in addition to fulfilling management tasks, contribute to the continuous optimization of these internal processes in line with a continuous improvement process. The Management Board is also supported in this by the internal audit department. Based on its review of the governance systems, the Management Board is unaware of any circumstances that would call into question the adequacy and effectiveness of these systems.

[1] The section "Statement on the adequacy and effectiveness of the governance systems" contains information outside the scope of the management report and was not subject to any substantive review by the auditor.

Description of the key features of the accounting-related internal control and risk management system pursuant to Section 289 (4) and Section 315 (4) HGB

The accounting-related internal control and risk management system within the secunet Group and secunet AG encompasses all principles, procedures, and measures to ensure the effectiveness, efficiency, and correctness of financial reporting and also guarantees compliance with applicable legal regulations. Risk identification and mitigation for the accounting-related internal control system (ICS) are carried out in the same way as for secunet's overall ICS.

Within the secunet Group, the internal control system consists of the internal management system and the internal monitoring system. The Management Board of secunet AG – with its corporate function of managing the business – has appointed the Risk Management department within secunet AG as the responsible body for coordinating the internal control system within the secunet Group.

Process-integrated and process-independent monitoring measures form the elements of the internal monitoring system within the secunet Group. In addition to manual process controls – such as the dual control principle – automated IT process controls are also an essential part of the process-integrated measures. Furthermore, process-integrated monitoring is ensured by bodies such as the Risk Committee and by specific Group functions such as the Legal Department. The internal audit department of secunet AG is integrated into the internal monitoring system of the secunet Group through process-independent audit activities.

The risk management system presented here is essentially aimed at preventing damage caused by risks.

Use of IT systems

The recording of accounting transactions within the secunet Group is primarily carried out using the ERP system from the manufacturer SAP.

Specific risks related to group accounting

Specific risks related to group accounting can arise, for example, from the conclusion of unusual or complex transactions, as well as from business transactions that are not handled routinely.

Key regulatory and controlling activities for ensuring the correctness and reliability of accounting within the Group

The control activities to ensure the correctness and reliability of financial reporting include, for example, the analysis of facts and developments using specific key performance indicator (KPI) analyses. The separation of administrative, operational, accounting, and approval functions, and their performance by different individuals, reduces the potential for fraudulent activities. Organizational measures are also designed to ensure that restructurings or changes in the business activities of individual business units are recorded promptly and appropriately in the consolidated financial statements. Furthermore, it is ensured, for example, that changes to the IT systems used for the underlying accounting in the group companies result in the accurate and complete recording of accounting transactions on a period-by-period basis. The internal control system is designed to also guarantee the reflection of changes in the economic or legal environment of the secunet Group and ensures the application of new or amended legal regulations for consolidated financial reporting.

The accounting regulations within the secunet Group, including the regulations for financial reporting in accordance with International Financial Reporting Standards (IFRS), govern the uniform accounting and valuation principles for the companies included in the consolidated financial statements of secunet AG.

The measures of the internal control system, which are geared towards the correctness and reliability of the consolidated financial statements, are designed to ensure that business transactions are recorded completely and promptly in accordance with legal and statutory requirements. Furthermore, it ensures that inventories are carried out properly and that assets and liabilities are correctly recognized, valued, and presented in the consolidated financial statements. The regulatory activities also ensure that reliable and traceable information is provided through the accounting records.

The German subsidiaries and the parent company prepare their annual financial statements in accordance with German commercial law. As part of the consolidation process, the financial statements are reconciled by the group accounting system to reflect the IFRS statement of financial position, as applicable in the EU. The consolidated financial statements are prepared through the consolidation of equity, liabilities, expenses, and revenues, as well as the elimination of intra-Group profits and losses in the consolidated statement of financial position and statement of profit or loss.

Restrictive notes

Despite the aforementioned internal organizational, control, and monitoring structures, personal discretion, flawed controls, criminal acts, or other unforeseen circumstances cannot be entirely ruled out. These can lead to limited effectiveness and reliability of the implemented internal control and risk management system, meaning that even the group-wide application of the system cannot guarantee absolute certainty regarding the correct, complete, and timely recording of events in the consolidated financial statements and the annual financial statements of the individual companies.

Takeover-related disclosures pursuant to Section 289a, sentence 1 and Section 315a, sentence 1 HGB

The Management Board of secunet AG provides the following information required under Section 289a, sentence 1 and Section 315a, sentence 1 HGB for financial year 2025:

1. The share capital of secunet AG remains unchanged at €6,500,000 and is divided into 6,500,000 no-par-value bearer shares. Each share grants one vote at the Annual General Meeting of secunet AG.

2. A restriction on the transfer of shares in secunet AG may arise from the German Foreign Trade and Payments Act (Außenwirtschaftsgesetz, AWG) due to the products offered by secunet AG. For example, Section 5 (3), sentence 1, no. 2 AWG stipulates that "restrictions may be imposed on the acquisition of domestic companies or shares in such companies by foreigners in order to safeguard essential security interests of the Federal Republic of Germany, if the domestic companies manufacture or have manufactured products with IT security functions for processing classified government information or components essential for the IT security function of such products and still possess the technology, provided that the overall product has been approved by the Federal Office for Information Security (BSI) with the knowledge of the company." Outside the restrictions of the Foreign Trade and Payments Act, the shareholders of secunet AG are not restricted in their decision to acquire or dispose of shares in the company by either German law or the company's Articles of Association. In particular, the acquisition and disposal of shares do not require the approval of the company's governing bodies or other shareholders to be effective. The voting rights of shareholders are not subject to any restrictions under either law or the company's Articles of Association. The Management Board is unaware of any agreements between shareholders that impose restrictions on the transfer of company shares.

3. According to the Management Board, 24.41% of the company's shares are publicly traded. Giesecke+Devrient GmbH, Munich, holds direct and indirect shareholdings exceeding 10% of the voting rights, with a direct shareholding of 75.12% as of December 31, 2025. MC Familiengesellschaft mbH, Munich, indirectly holds a 75.58% share in secunet AG through its shareholding in Giesecke+Devrient GmbH (including the shares held by secunet AG itself). Verena von Mitschke-Collande, Celia von Mitschke-Collande, Marian von Mitschke-Collande, Sylvius von Mitschke-Collande, and Gabriel von Mitschke-Collande also hold a 75.58% share in secunet AG indirectly through MC Familiengesellschaft mbH.

4. secunet AG has not issued any shares that grant special rights.

5. Like all other shareholders of the company, the employees and members of the Management Board who hold shares in the company's capital decide on the exercise of their voting and control rights themselves and therefore exercise their control rights directly.

6. The Management Board of secunet AG is appointed and dismissed in accordance with statutory provisions, in particular Sections 84 and 85 of the German Stock Corporation Act (AktG). The Articles of Association do not contain any special provisions for the appointment and dismissal of individual or all members of the Management Board. The Supervisory Board alone is responsible for their appointment and dismissal. It appoints Management Board members for a maximum term of five years. Reappointment or extension of the term of office, each for a maximum of five years, is permitted. Amendments to the Articles of Association require a resolution of the General Meeting pursuant to Section 179 of the German Stock Corporation Act (AktG), whereby amendments that only affect the wording may also be delegated to the Supervisory Board. The amendment becomes effective upon registration in the Commercial Register. According to Article 22 of the Articles of

Association, resolutions of the General Meeting require a simple majority of the votes cast, unless the Articles of Association or mandatory provisions of law stipulate otherwise. Article 10 (5) of the Articles of Association authorizes the Supervisory Board to resolve amendments to the Articles of Association that only affect the wording.

7. The Management Board is not authorized to issue new shares. Neither the Articles of Association of secunet AG provide for a conditional capital increase, nor is the Management Board authorized to increase the share capital by issuing new shares against contributions (authorized capital). There is also no authorization to acquire treasury shares pursuant to Section 71 (1), no. 8 of the German Stock Corporation Act (AktG). As of December 31, 2025, the company held 30,498 treasury shares, which it had acquired based on an authorization granted by the Annual General Meeting on May 29, 2001. By resolution of the Annual General Meeting of May 27, 2009, the Management Board was authorized to sell these shares on a stock exchange with the approval of the Supervisory Board. The Management Board of secunet AG did not make use of this authorization by December 31, 2025.

8. There are no material agreements of the company that are subject to a change of control as a result of a takeover bid.

9. No compensation agreements were made with any member of the Management Board or employees of the company in the event of a takeover bid.

Management and control – reference to the Corporate Governance Statement pursuant to Sections 289f and 315d HGB

As a German stock corporation, secunet AG has a dual management and control structure. The Company and the Group are managed by the Management Board, whose members are appointed by the Supervisory Board. The Supervisory Board advises the Management Board and oversees its management.

A more detailed analysis of the management of the secunet Group can be found in the Corporate Governance Statement pursuant to Sections 289f and 315d of the German Commercial Code (HGB), which is made available in this annual report and on the corporate website (www.secunet.com) under >> About Us >> Investors >> Corporate Governance.

The information in the Corporate Governance Statement is not included in the annual and consolidated financial statement audit in accordance with Section 317 (2), sentence 6 of the German Commercial Code (HGB).

(Combined) Sustainability Statement

With this (Combined) Sustainability Statement (hereinafter referred to as the Sustainability Statement), secunet fulfills the Company's and the Group's obligation to disclose non-financial information for the 2025 financial year. In doing so, we comply with the "Act to Strengthen Non-Financial Reporting by Companies in their Management Reports and Group Management Reports (CSR Directive Implementation Act, CSR-RUG)" pursuant to Sections 315b, 315c in conjunction with Sections 289b – 289e of the German Commercial Code (HGB) and Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 establishing a framework to facilitate sustainable investment and amending Regulation (EU) 2019/2088.

The Sustainability Statement outlines how environmental, social, and governance (ESG) impacts, risks, and opportunities are managed within the secunet Group. This approach is based on Directive (EU) 2022/2464 on corporate sustainability reporting, also known as the Corporate Sustainability Reporting Directive (CSRD). The sustainability statement requires companies to include information in their management report that is necessary for understanding the impact of the company's activities on sustainability aspects, as well as the impact of sustainability aspects on the company's business performance, results of operations, and financial position.

Since the European Commission has adopted the European Sustainability Reporting Standards (ESRS) as reporting standards, this year's reporting is carried out in full compliance with the ESRS (European Sustainability Reporting Standards) as a framework pursuant to Sections 315c (3) in conjunction with 289d of the German Commercial Code (HGB). This sustainability statement in accordance with the ESRS also fulfills the requirements for the non-financial (combined) statement prepared pursuant to Sections 315b to 315c in conjunction with 289b to 289e of the German Commercial Code (HGB).

The following conversion table clarifies which ESRS cover the requirements of Section 289c (3) of the German Commercial Code (HGB).

Reconciliation of ESRS matters/disclosures concerning aspects in accordance with Section 289c (3) HGB:

Aspect according to Section 289c (3) HGB	ESRS according to CSRD
Environmental concerns	ESRS E1
	ESRS E5
Employee concerns	Aspects from ESRS S1
	Aspects from ESRS S2
Human rights	Aspects from ESRS S1
	Aspects from ESRS S2
Social issues	Aspects from ESRS S2
Avoidance of corruption and bribery	ESRS G1
General disclosures	n/a

The information in the sustainability statement is not included in the audit of the combined management report in accordance with Section 317 (2), sentence 4 of the German Commercial Code (HGB). Instead, the combined Sustainability Statement of the Company and the Group was audited by BDO AG Wirtschaftsprüfungsgesellschaft in accordance with the requirements of auditing standard ISAE 3000 (Revised) with a "Limited Assurance".

This Sustainability Statement, together with the combined Management Report – report on the situation of the Company and the Group – is made publicly available on the corporate website (www.secunet.com) in the section >> About us >> Investors >> Financial publications.

Contents index

ESRS 2 General Disclosures

ESRS E1 – Climate Change

ESRS E5 – Circular Economy and Resource Use

EU Taxonomy

ESRS S1 – Own Workforce

ESRS S2 – Workers in the Value Chain

ESRS G1 – Business Conduct

Company-Specific Matters

ESRS 2: General disclosures

1. Basis for preparation

BP-1: General basis for preparation of the sustainability statement

The (Combined) Sustainability Statement 2025 (hereinafter referred to as the Sustainability Statement) was prepared on a consolidated basis. The companies included in the consolidated Sustainability Statement are the same as those included in the scope of consolidation in the consolidated financial statements. If individual subsidiaries that are part of the scope of consolidation are not included in specific sections of the combined Sustainability Statement, this is indicated separately in the relevant sections of the Sustainability Statement.

In our sustainability activities and in assessing the impact of the secunet Group (secunet) on sustainability aspects, we consider our own business operations as well as the upstream and downstream value chain. Accordingly, we include the upstream and downstream value chain in our sustainability statement wherever possible. Due to limited information and data available on the upstream and downstream value chain, it is not possible to consider it in all reporting standards where this is required. We make this transparent in this report under the respective matters.

secunet has not made use of either the safeguard clause pursuant to ESRS 1, Chapter 7.7 (Classified and sensitive information, and information on intellectual property, know-how or results of innovation) or the safeguard clause pursuant to CSRD with regard to information on forthcoming developments or matters under negotiation in the preparation of this sustainability statement.

BP-2: Disclosures in relation to specific circumstances

secunet provides the following information regarding specific circumstances of its sustainability reporting. Any deviations from the information presented here will be disclosed and explained in the relevant sections of the Sustainability Statement.

- The Company has not deviated from the medium- or long-term time horizons set out in ESRS 1 Section 6.4 for reporting purposes. Accordingly, we have established the following time intervals:
  - For the short-term time horizon: the current financial year (calendar year),
  - for the medium-term time horizon: from the end of the short-term reporting period up to five years and
  - For the long-term time horizon: more than five years.
- Our Sustainability Statement includes various estimates of data on the upstream and downstream value chain data when calculating CO_2 emissions for the determination of Scope 3 emissions (3.1), which are calculated using the spend-based approach. These parameters and monetary amounts are disclosed and explained in the relevant sections of the report.
- Our Sustainability Statement does not mention any metrics or monetary amounts that are subject to measurement uncertainty.
- Unless otherwise stated, the metrics have not been validated by any other external body.
- This Sustainability Statement is the second to comply with the reporting requirements of the CSRD and thus the ESRS. The following changes must be reported compared to the first statement:
  - The double materiality assessment has been updated. This did not yield any significant new findings regarding the matters material to secunet. Primarily, redundancies among the IROs were eliminated. A few IROs were reassessed. Further details can be found in the relevant section of this report.
  - The 2024 report incorrectly stated under E1 that 100% green electricity was used and under E5 that no hazardous waste was generated. Both statements were subsequently identified as incorrect and corrected accordingly in the current reporting year.

- In this Sustainability Statement, secunet does not include any information based on other legal regulations that require the company to disclose sustainability information, or on generally accepted standards and frameworks for sustainability reporting. Accordingly, such information is not to be reported.
- secunet does not include any information by reference in this Sustainability Statement. Therefore, such information is not to be reported.
- The provisions for phased disclosure requirements according to ESRS 1 Annex C do not apply to secunet. Accordingly, information on this is not included in our Sustainability Statement.

2-Governance

GOV-1: The role of the administrative, management and supervisory bodies

secunet Security Networks AG is subject to German stock corporation and capital market law as well as the rules of its own Articles of Association. As a German stock corporation, it has a dual management and control structure, reflected in its Management Board and Supervisory Board.

The Management Board and Supervisory Board work closely and collaboratively in managing and overseeing the company. The general meeting is responsible for fundamental company decisions.

The Management Board, as the governing body, manages the company's affairs independently and in the company's best interests, and represents the company. Its focus is on the sustainable increase of the company's value. In particular, it establishes the principles of corporate policy and is responsible for the company's strategic direction, the planning and setting of the corporate budget, resource allocation, and the control and management of the company and its segments. Certain measures, as described in the Management Board's rules of procedure, require the approval of the Supervisory Board. The Management Board is responsible for preparing the company's quarterly and semi-annual financial reports, the annual financial statements of secunet Security Networks AG, and the consolidated financial statements.

The Management Board informs the Supervisory Board regularly, promptly, and comprehensively in written and oral reports about all matters relevant to the company as a whole, including strategy and strategy implementation, planning, business development, the financial performance and results of operations, and entrepreneurial risks. The Supervisory Board is directly involved in all decisions of fundamental importance to the company.

The Supervisory Board oversees and advises the Management Board in the management of company. At regular intervals, the Supervisory Board discusses business development and planning, as well as strategy and its implementation. It reviews the semi-annual financial reports and quarterly statements with the Management Board before their publication and approves the annual financial statements of secunet Security Networks AG and the Group, taking into account the auditor's reports, the preliminary review by the Audit Committee, and its own review. The Audit Committee oversees the accounting process, the effectiveness of the internal control system, risk management, the compliance management system, and internal audit, as well as the final audit.

The company's Management Board comprises four members, including one woman, resulting in a ratio of 1:3 and a 25% female-to-male representation. The Supervisory Board consists of six members, two of whom are appointed as employee representatives under the One-Third Participation Act. The Supervisory Board also includes one woman, representing 16.7% of its members.

The members of the Management Board and the Supervisory Board bring a wide range of experience and expertise to the company. The Supervisory Board has defined objectives for its composition with regard to both diversity and professional competence (knowledge, skills, and professional experience), which have been summarized in a competency profile. The members of the Management Board possess comprehensive expertise in their respective areas of responsibility, gained through their many years of professional experience. Both the Supervisory Board and the Management Board include members with experience working abroad.

Individual members of the Management Board and the members of the Supervisory Board's Audit Committee have acquired expertise related to sustainability through various means:

- Training on sustainability matters and regulatory requirements, also with regard to reporting.
- Advice from experts, e.g., auditors.
- Several years of supporting the sustainability reporting of secunet Security Networks AG and the experience gained in the process.

This expertise fosters an understanding of the risks and opportunities arising from a sustainability perspective and supports future-oriented action within the company.

The independence of the committee members is another crucial aspect, as it strengthens objective decision-making and oversight. The Supervisory Board of secunet Security Networks AG meets all the requirements of the German Corporate Governance Code (DCGK) regarding the independence of its members. The proportion of independent members is 16%.

The Supervisory Board is responsible for monitoring the impacts, risks, and opportunities of sustainability. This responsibility lies with the Audit Committee, which deals with sustainability issues and sustainability reporting, and with the entire Management Board of secunet Security Networks AG, which is informed about sustainability matters as needed. Responsibilities for individual impacts, risks, and opportunities are assigned within the Management Board according to the distribution of responsibilities. The execution of these tasks is delegated to the respective departments. For example, the CEO, who is responsible for HR, is responsible for issues related to ESRS S1 "Own Workforce." The implementation of these tasks is then the responsibility of the Head of HR.

ESRS	Department	Board responsibility
2 General disclosures	Sustainability	CFO
E1 Climate change	Environmental management	COO
E5 Circular economy	Sustainability	CFO
S1 Own workers	HR	CEO
S2 Workers in the value chain	Compliance	CFO
G1 Business conduct	Compliance	CFO
Company-specific: Information security	Product strategy, product management	CTO

The management has delegated the tasks of monitoring and controlling impacts, risks, and opportunities, as well as the responsibility for internal and external reporting, to the Sustainability department. No specific controls or procedures are in place for managing impacts, risks, and opportunities (IROs).

Setting targets, where possible, is part of the Management Board meetings, during which the discussion and approval of sustainability-related activities (or the ESG strategy) is on the agenda. Remuneration-related targets are submitted to the Supervisory Board for approval.

GOV-2: Information provided to and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies

The Management Board and Supervisory Board are regularly informed once a year about significant impacts, risks, and opportunities. This information includes a description of the current status of the Double Materiality Assessment (DMA), including any changes, the procedures for identifying and assessing the impacts, risks, and opportunities, as well as the status of implementation and any changes to the ESG strategy. If necessary, that is, primarily when significant changes are being discussed or when decisions need to be made, further consultations take place beyond this regular information.

The Management Board and Supervisory Board discuss the effects of impacts, risks, and opportunities related to the company's strategy, major transactions, and risk management as an integral part of their decision-making processes during board meetings, provided these effects are material. When making strategic decisions and transactions, secunet's governing bodies analyze whether and to what extent compromises are necessary with regard to other strategic aspects. In particular, they assess whether the decision is consistent with the long-term targets of the sustainability strategy.

For the year 2025, the Supervisory Board was informed about the changes to the impacts, risks, and opportunities and the associated changes to the Double Materiality Assessment (DMA), as well as the impact on the ESG strategy. This information resulted from the presentation of the material aspects of the 2025 Sustainability Statement, the audit of which by the external auditors was reported.

GOV-3: Integration of sustainability-related performance in incentive schemes

Sustainability-related targets and performance metrics are part of the long-term variable compensation of the Management Board of secunet AG. Accordingly, sustainability is included in the long-term variable compensation of the Management Board as a performance criterion with a weighting of generally 30% (share of the long-term variable compensation).

The Supervisory Board defines various sustainability and ESG targets annually, usually up to three. These may include, for example, diversity targets within the workforce, securing future talent and the attractiveness of secunet AG as an employer, occupational health and safety, and training and development targets. Compliance with environmental regulations or the establishment and maintenance of compliance structures may also be included in the performance category.

Progress on the relevant measures regarding the key annual sustainability targets is assessed annually (particularly based on a sustainability statement), and the performance of each Management Board member is evaluated on a scale of 50% to 150%, with the aim of ensuring measurable target achievement wherever possible. Where measurable target achievement is not possible, the Supervisory Board determines the target achievement for all sustainability/ESG targets at its own discretion. If the minimum performance of 50% of the set sustainability targets is not met, the target achievement is 0%. Exceeding the 150% threshold is not permitted.

Specifically, the portion of the variable remuneration of the Management Board of secunet Security Networks AG that is linked to ESG targets is structured as follows for the year 2025:

- Reduction of CO_2 emissions by secunet Security Networks AG. Climate-related considerations are thus included in the remuneration.
- Percentage of women among the managers in the secunet Group.
- Increased customer satisfaction, as measured by the Net Promoter Score (NPS).

Background information on the calculation can be found in the remuneration report of secunet Security Networks AG.[2]

The remuneration of the Supervisory Board of secunet Security Networks AG has no connection to climate-related considerations or other sustainability-related aspects.

GOV-4: Statement on due diligence

The core elements of due diligence regarding both human and environmental impacts can be compared with the relevant information listed below in secunet's Sustainability Statement.

[2] The Management Board's ESG compensation targets for 2025 do not align with the targets formulated for the ESG strategy. This is primarily because the strategy-relevant targets were only specified in detail during 2025. For the years 2026 and beyond, a high degree of alignment is the goal.

Key elements of due diligence	Disclosures in the Sustainability Statement
a) Integrating due diligence into governance, strategy and business model	GOV-1 Management of responsibilities GOV-1 Monitoring of sustainability IROs GOV-2 Information provided and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies GOV-3 Integration of sustainability-related performance in incentive systems SBM-3 Double Materiality Assessment
b) Involvement of affected stakeholders in all key due diligence steps	SBM-2 Stakeholders' interests and positions GOV-2 Information provided and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies IRO-1 Double materiality assessment process
c) Identification and assessment of negative impacts	SBM-3 Double Materiality Assessment SBM-3 Results of the Double Materiality Assessment IRO-1 Double materiality assessment process
d) Actions to counter these negative effects	E1-3 Actions and resources in relation to climate change policies E5-2 Actions and resources related to resource use and circular economy S1-4 Actions S2-4 Actions G1-2 Management of relationships with suppliers G1-3 Prevention and detection of corruption and bribery
e) Tracking the effectiveness of these efforts and communication	S1-4 Actions S2-3 Processes to remediate negative impacts and channels for value chain workers to raise concerns G1-1 – Policies

GOV-5: Risk management and internal controls over sustainability reporting

Risk management and internal controls relating to sustainability reporting are based on the risk management and internal control system (ICS) used at secunet (see the corresponding explanation in the Management Report). Since sustainability reporting is a recurring process, process risks are mitigated according to the ICS principles. Risk identification and assessment are based on many years of experience with various types of reporting (Management Report, Non-Financial Statement, Sustainability Statement). Prioritization of risks is not necessary due to the manageable number of material risks.

Based on this, secunet identifies incomplete, inaccurate, and untimely reporting as the main risks of sustainability reporting. Organizational measures have been implemented to mitigate these risks.

Risk management system and internal control system with regard to sustainability reporting

Risks	Mitigated by
Late reporting	Centralized coordination by the Sustainability department, scheduling and ongoing monitoring
Incorrect information in the individual ESRS	Each department is staffed with two people to review the information.
Incorrect KPIs	Data is entered into the Sphera IT system at the parent company G+D using the six-eyes principle at secunet (entry, approval, and validation), and plausibility is checked by G+D. The data is then transferred from Sphera to the IT system for secunet reporting; this is followed by a further check for transmission errors.

The sustainability reporting for the entire Group is coordinated by the Sustainability department of secunet Security Networks AG. Detailed scheduling and ongoing monitoring of deadlines prevent late reporting.

Through the intensive involvement of the specialist departments and the ongoing monitoring of the Sustainability Statement's content (comparison with the ESRS requirements) by the Sustainability department, the risks of incomplete and inaccurate reporting are mitigated. This form of management was implemented throughout the entire financial year to identify the Sustainability Statement's content well in advance and to close any potential gaps.

In addition, a preliminary review by the auditors commissioned with the audit takes place prior to the main audit of the sustainability report. This largely prevents potential deficiencies. Furthermore, the risk of incomplete documentation and evidence is avoided by the audit.

The Sustainability department regularly informs the Management Board of secunet Security Networks AG about the status of the Sustainability Statement preparation in light of the aforementioned risks. During the report preparation phase, this information is provided monthly, and during the finalization phase, weekly. To mitigate risks, ongoing consultations are held with the auditors, and a summary report is submitted to the Management Board based on these consultations.

3-Strategy

SBM-1: Strategy, business model and value chain

secunet is one of the leading cybersecurity companies in Germany. In an increasingly interconnected world, the company combines products and consulting services to create resilient digital infrastructures and provide the highest possible level of protection for data, applications, and digital identities. A key component of its portfolio is network components featuring advanced encryption technologies, approved by the German Federal Office for Information Security (BSI) up to the highest national security level.

secunet's business covers the entire value chain, from analysis and design through development to integration, operation, maintenance, and support of solutions. The extensive use of open-source software and a multitude of coordinated security mechanisms enable the realization of flexible, scalable, and highly secure solutions. These are typically tailored to specific application scenarios in industries with particularly high information security requirements.

A key component of the product range is the IP-based cryptosystem SINA ("Secure Inter-Network Architecture"), developed in cooperation with the German Federal Office for Information Security (BSI). SINA protects electronic information from unauthorized access and enables the secure processing, storage, and transmission of classified information via the internet. With BSI approvals up to the highest national security classification of SECRET, SINA meets maximum security standards.

The SINA product family comprises a constantly growing number of modular components such as clients, gateways, servers, and software tools. These components are used to secure a wide variety of application scenarios. Special SINA components are offered for high-security military and government networks, which place particularly high demands on data security and equipment resilience. These are based on a hardened hardware platform and are designed for extreme operating conditions. Since 2025, secunet has also been offering the SINA Cloud, a solution for the legally compliant processing of highly sensitive and classified information (confidential documents).

Key product offerings also include activities in the areas of digital identities and biometrics. These offerings encompass solutions for personal identification and user authentication on web portals, as well as biometric capture and verification in connection with official identity documents. This also includes automated border control systems that ensure a smooth and secure flow of passengers at airports and other border control points.

In the healthcare market, secunet targets its services at medical providers, including physicians, hospitals, and pharmacies. The core of its offering lies in providing various connectors. These connectors offer secure access to the telematics infrastructure (TI) and provide interfaces to applications such as the electronic patient record (EPR) and the electronic prescription (ePrescription). Additionally, the connectors perform crucial security functions, such as encrypting and signing medical documents. This ensures the secure transmission and processing of sensitive health data within digital healthcare applications.

For industry, secunet offers solutions for secure edge computing as well as early warning systems for the prevention and detection of cyberattacks. The focus is particularly on manufacturing companies with high security requirements. Critical infrastructures (KRITIS) are also addressed, meaning organizations and facilities of vital importance to the functioning of society, including those in the energy, transport, water, finance, and insurance sectors.

secunet is not active in the fossil fuel sector, nor in the manufacture of chemicals, nor in the field of controversial weapons, nor in the cultivation and production of tobacco.

Reporting according to ESRS sectors is not yet mandatory at the time of preparation of this Sustainability Statement.

There are no prohibitions on secunet's products or services. There are only restrictions regarding eligible customers and regions for products subject to export restrictions, foreign trade regulations, and national confidentiality. These primarily include products in the SINA product family.

secunet's sales focus is primarily in Germany. Its international sales activities concentrate on countries within the European Union, EU organizations, defense and space agencies (including organizations such as NATO), and the Middle East.

secunet's customers are primarily from the public sector, including national and international governments, ministries, and agencies, as well as quasi-governmental organizations. The German Armed Forces and defense organizations, along with security agencies such as police and border patrols, are also key clients. The Company also serves sectors with specific IT security requirements, such as healthcare and industry.

secunet's business model is based on specific inputs that are collected, developed, and secured in the following way: A distinction is made between development services/software and hardware on the one hand (IT solutions) and the consulting business provided by secunet's employees on the other hand:

- IT solutions: Hardware requirements are met through centralized purchasing and supply chain management, while software development services are primarily provided by in-house staff. These needs are met through employee development and recruitment.
- Consulting business: Here too, needs are met through employee development and recruitment.

The outputs of secunet's business model and the results regarding current and expected benefits for customers and investors are:

- Outputs to customers include solutions and IT products, software and IT hardware, as well as consulting services.
- Outputs to investors include information from regular financial and non-financial reporting or from investor discussions. Furthermore, investors receive returns through dividend payments from annual profits and through increases in share value.
- There are no other significant stakeholders who receive outputs from secunet's business model.

secunet does not have a dominant market position within the value chain:

In the upstream value chain, IT hardware is procured. secunet has a heterogeneous supplier structure, including both medium-sized and large players in the standard IT hardware sector. Suitable personnel are also recruited in the upstream value chain. secunet competes with many other (IT) companies for qualified personnel.

In the downstream value chain, two types of markets can be distinguished. Firstly, there are regulated markets where only approved or certified products can be traded. secunet has a strong market position here, as many products in its portfolio have received approval. The situation is different in unregulated markets, where competition is significantly higher. Here, secunet competes with national and international suppliers.

As of December 31, 2025, secunet employs a total of 1,302 people, all of whom are based in Germany.[3]

SBM-2: Stakeholders' interests and positions

Our stakeholders and interest groups include our customers, business partners, employees, investors and analysts, legislators and associations, employees in the value chain, affiliated companies and cooperation partners, NGOs, and all those in politics, business and society interested in the sustainable practices of secunet AG.

As part of its stakeholder analysis, secunet identified internal and external stakeholders, sorted them by relevance, and evaluated them. The stakeholder analysis was discussed and validated with the relevant departments dealing with the respective stakeholders and with the Management Board.

We maintain an active stakeholder dialogue across all our business activities, utilizing various channels and activities to engage stakeholders. The form of this dialogue depends on the topic and the stakeholders involved, as not every stakeholder can be considered equally relevant to every aspect of our strategy, including sustainability.

[3] Excluding the Management Board.

Due to their experience and operational responsibilities, the Management Board and Supervisory Board are already informed about the positions and interests of the stakeholders concerned. If this information needs to be supplemented with current sustainability issues, appropriate notification will be issued.

Key stakeholders	Organization of the engagement	Purpose and outcome of the engagement
Employees	› Formal employee meetings; › Identifying training needs and implementing them; › Workshops; › Works meetings; › Works council (syseleven) › All-hands meetings; › Site visits with dialogue format.	› Offer attractive employment and career opportunities; › Develop skills, talents and experience; › Promote diversity, equal opportunities, inclusion, belonging and corporate culture.
Customers	› Direct exchange in regular customer and project business, e.g. via key account managers; › BSI's collection and reporting of customer feedback in the public sector; › Regular customer events; › Customer survey with top ten customers per division, including questions about good/bad experiences with secunet (products), plus the option for plain-text comments. The collected data will be forwarded to the relevant divisions.	› Improve customer satisfaction and expand product and service offerings.
Suppliers & business partners	› Supplier discussions; › Supplier reviews; › Supplier audits; › Bilateral exchange.	› Create mutually beneficial economic value for our suppliers and partners; and › Ensure an environmentally and socially responsible supply chain. We want to work with suppliers who share the same values and are committed to improving sustainable practices.
Investors & analysts	› Year-round dialogue through investor relations events and meetings; › Regular discussions with analysts and investors; › Annual General Meeting.	› Create a good understanding of the economic situation of secunet AG and to promote the company's prospects for generating total shareholder return through share price increases and dividends.
Affiliated companies & cooperation partners	› Direct exchange with affiliated companies; › Strategic alignment	
Workers in the value chain	› Exchange with suppliers on topics relating to workers in the supply chain	

Through various well-established dialogue formats, the perspectives of employees are incorporated into the strategies, decisions, and actions of the secunet Group. Stakeholder interests are included in the materiality assessment and determine its outcome.

- Regular dialogues between employees and their managers (e.g., annual target agreement and target achievement discussions as well as interim discussions)
- Exchange formats between the Management Board and employees (e.g., all-hands meetings; secublog)
- Staff meetings
- Exchange, consultations and negotiations between the Management Board and the HR department
- Employee surveys: Measuring employee satisfaction. This survey provides insights into employee satisfaction and motivation, the quality of collaboration, and changes in corporate culture. By allowing open-ended responses in the surveys, we also encourage employees to provide concrete suggestions for improvement, from which we derive actions to optimize our performance as an employer. The results of the employee surveys also serve as a basis for regular dialogue between managers and employees in the various departments and units of our Company.

The interests, viewpoints and rights of workers in the value chain who may be significantly affected by secunet, including respect for their human rights, are taken into account.

The foundation of secunet AG's purchasing and procurement process is clearly defined procedures and responsibilities, firmly anchored in the company's process landscape. Annual discussions are held with secunet AG's key suppliers to review their internal supplier evaluations and discuss potential or necessary changes, including sustainability issues. The goal of these discussions is to foster positive supplier development and ensure a consistently positive evaluation. We observe that many of our suppliers are already on the path to sustainable development or have already implemented it.

Our procurement platform includes a supplier questionnaire that provides a detailed profile of the supplier. One section of the questionnaire addresses the German Supply Chain Due Diligence Act (LkSG), inquiring about the company's positions on human rights issues and fundamental sustainability aspects. The supplier evaluation is based on the questionnaire responses and an abstract risk analysis that considers industry and country risks.

SBM-3: Material IROs and their interaction with strategy and business model

Our identified material IROs are outlined in the DMA process (Double Materiality Assessment) and further described in the respective topic-specific sections. The material IROs are derived from and congruent with secunet's business model and strategy. Therefore, no changes to the business model or strategy are planned as a result of the IROs.

Overall, our material IROs relate to the core activities of our business model and focus primarily on our own operations. Because our material IROs are closely linked to our business model, we manage most of them directly as part of our ongoing business activities. This applies particularly to governance IROs and our own workforce. For environmental IROs identified in our upstream and downstream value chain, our direct influence lies in strengthening processes, especially in procurement and waste management.

Our main environmental impacts result primarily from CO_2 emissions. However, these emissions are low due to our business model. Detailed information on resilience to specific climate risks, including climate risk analysis, can be found in the below sections of the report on ESRS E1.

The identified negative social impacts are potential in nature and arise primarily from industry-specific challenges such as data protection and high workloads. To address these challenges, we have implemented targeted actions and guidelines. If these actions are not continued, the potential negative impacts on employees and customers could spread.

As an IT service provider, we also make a positive contribution: We invest specifically in the further training and skills development of our employees and promote social standards within our own workforce. Through the protection of digital infrastructures, secunet supports digitalization in society – especially for public institutions.

Current financial impact

The financial impact of the identified material risks and opportunities is currently limited. Resource expenditure for compliance with the CSRD and the EU Taxonomy remains at a similar level to the previous year. The number of employees in this area has also remained the same. Based on our increased experience, our investments in external consulting services for CSRD implementation in 2025 have decreased.

Since our material IROs are closely linked to our core activities and growth potential, actions to optimize opportunities and mitigate risks and negative impacts are embedded in our existing governance structures. This enables us to demonstrate a high level of resilience within the time horizons defined for the 2024 and 2025 DMAs. This assessment is based on qualitative analyses by internal experts who conducted a holistic evaluation of existing risk mitigation measures for all IROs as part of the DMA process.

Sustainability risks and opportunities are not prioritized over other risks and opportunities within secunet's risk management.

Changes in material IROs

The DMA 2025 did not introduce any significant new topics compared to the DMA 2024 – the reported ESRS remain the same. Due to growing experience with the CSRD, the DMA 2025 resulted in a smaller number of IROs. This is primarily due to the consolidation of redundant IROs. Additionally, some IROs fell below the materiality threshold after their assessment was reviewed.

4-Management of IROs

IRO-1: Description of the of the process to identify and assess material impacts, risks and opportunities

Background and methodology of the DMA

Since 2023, we have conducted a double materiality assessment (DMA) annually and report on it in our sustainability statements. Our sustainability reporting is based on the CSRD (Directive (EU) 2022/2464) and the ESRS. The methodology for assessing material IROs has been continuously developed to meet the CSRD requirements. Our DMA is based on the findings of previous years, with the results of the 2024 materiality assessment being reviewed again to ensure their continued relevance and accuracy. This review considered our business model, stakeholders, value chain, and existing dependencies. In this context, the perspectives and interests of the stakeholders involved were also incorporated through the assessment of the relevant departments. The stakeholder analysis served as the basis for identifying material impacts, risks, and opportunities.

The DMA is conducted in accordance with the double materiality principle. This principle states that disclosures on ESG issues are required if material impacts on people and the environment (impact materiality) or financial effects on the company (financial materiality) have been identified. To identify potentially material issues and their impacts, risks, and opportunities, either a top-down or bottom-up approach can be used. In our case, the top-down approach was used, based on the ESRS.

Conducting the materiality assessment

The following methodological and content-related changes were made during the revision of the materiality assessment 2024 to create the materiality assessment 2025:

While the materiality assessment for 2024 was still conducted using the spreadsheet program Excel, the materiality assessment for 2025 was implemented using the functionalities of the (risk management) tool Schleupen GRC. In Schleupen GRC, IROs can be documented and assessed: the parameters (assessment configurations) proposed by EFRAG for IRO assessment can be set for this purpose. In this respect, the consideration of IROs from the materiality

assessment is integrated into secunet's risk and opportunity management: the same tool is used, only the approaches to the assessment differ.

From summer 2025 onwards, the results of the 2024 materiality assessment were validated and the parameters for determining the 2025 materiality assessment were defined. The following questions were asked for each IRO:

- Is the IRO still relevant? If not, it has been deactivated.
- Is the IRO possibly redundant? IROs with similar meanings have been merged into one, and the remaining one has been deactivated.
- Does the assessment still reflect the previous status? The assessment parameters for the IROs were reviewed and corrected where necessary.

The materiality assessment took place in discussions between the sustainability team and the specialist departments.

Evaluation system

The assessment of materiality is carried out in two dimensions:

- **Impact Materiality:** Determining the materiality of impacts on humans and the environment based on the following criteria:
  - Extent: Intensity of the impact
  - Scope: Reach of the impact (affected persons or resources)
  - Reversibility (in case of negative effects): Possibility of counteracting the effects.
  - Probability of occurrence: The likelihood of occurrence within the next ten years

Impact materiality is calculated using the formula:

Impact Materiality = Severity of impact x Probability of occurrence.

The severity of the (negative) impact is the sum of its magnitude, extent, and reversibility.

- **Financial Materiality:** Determining financial opportunities and risks by including the following criteria:
  - Probability of occurrence: Assessment of the risk before taking countermeasures
  - Significance of financial impact: Assessment of the potential damage or gain from ESG issues

Financial materiality is calculated using the formula:

Financial Materiality = magnitude of financial impact x probability of occurrence.

An ESG issue is considered material if its rating is between 3 or -3 and 5 or -5.

In identifying and assessing the risks and opportunities, we also considered interactions with their impacts. This means that we not only looked at the risks and opportunities that were immediately apparent, but also whether and to what extent the impacts would create long-term risks and opportunities.

Validation and release

The materiality assessment was initially conducted by the Sustainability department and subsequently validated in separate discussions with the relevant specialist departments. The results were discussed from two perspectives to compare the assessments and make adjustments where necessary. Following this internal review, a comprehensive analysis was conducted to identify any discrepancies and implement necessary changes. The final results were presented to the Management Board in January 2026, and final approval was granted on February 6, 2026.

Updates and adjustments

The Materiality Assessment (DMA) is reviewed annually and updated as needed, taking into account new data or insights. Changes in influencing factors and new regulatory requirements are considered. Changes to the procedure compared to the previous reporting period are explained above. The materiality assessment will be reviewed again during financial year 2026 to prepare for the 2027 sustainability reporting. In addition, non-material data points were also assessed. This involved analyzing the objective and content of the respective requirements, their relevance to our business, and their potential benefits for users of our annual report.

Where possible, existing quantitative data from secunet's internal accounting or from valid sources on the internet or other media were used as data sources for the evaluation. Assumptions were checked for plausibility with the relevant departments where possible and necessary.

Environment

As part of our comprehensive analysis process, we used a combination of internal dialogue and the expertise of our environmental management team to thoroughly assess our current situation. We concluded that while our Company does have an impact on climate change, this impact is considered minor due to our greenhouse gas footprint.

No consultations, particularly with affected communities, were conducted.

E1

To complement our DMA, we conducted a climate risk analysis. This provided us with a sound understanding of our current situation. In this context, we also examined the extent to which future scenarios might reveal potential additional risks for our Company, including our business activities and assets. Based on this scenario-based assessment methodology, no material additional risks beyond those already reported above could be identified.

Aspect	Description
Object of investigation	secunet Group (Germany), primarily office buildings, no significant manufacturing activities. Focus on climate risks to its own business operations and indirect effects in the value chain.
Time horizon	The observation period is 5 to 25 years, with an endpoint around 2050.
Climate change scenarios	Best Case (Net Zero Emissions 2050): Strict climate policy, rapid technological progress, renewable energies, no new coal or natural gas projects. Worst Case (SSP5-RCP8.5): Temperature increase of 4°C, extreme weather events, rising sea level, heavy use of fossil fuels.
Stakeholder engagement	Interviews with departments such as Supply Chain Operations, Central Purchasing, HR, Facility Management, CIO and CISO for risk assessment.

As part of the DMA (Double Materiality Assessment) and the associated analyses, we considered climate-related hazards and transition risks in accordance with the applicable application requirements in the field of climate change. Our current assessment approach allows for an appropriate evaluation of our situation, particularly since potential risks are considered limited. Nevertheless, we will continuously examine to what extent further analyses, such as more detailed scenario analyses, could provide additional value to our assessments.

E2

To determine the actual and potential impacts, risks, and opportunities of secunet related to environmental pollution within its own operations and its upstream and downstream value chain, the environmental management, central product management, and product compliance departments were surveyed in close conjunction with the materiality assessment. Their responses were incorporated into the assessment that environmental pollution is not material to secunet.

E3

Since secunet's business model and its own activities, as well as the activities within the upstream and downstream value chain, have no known or suspected points of contact with water and marine resources, the ESRS E3 was assessed as not material.

E4

To determine whether the activities at secunet's sites have an impact on biodiversity and ecosystems, a biodiversity analysis and discussions with the Facility Management and Environmental Management departments were carried out.

The biodiversity analysis was conducted in 2024; the methods and results remain valid. The analysis involved examining all 13 secunet sites for the presence of protected areas or Key Biodiversity Areas (KBAs) within a 5 km radius, using specialized geodata services and biodiversity tools. The analysis revealed that 7 of the 13 sites contain protected areas or KBAs; however, no material impacts of the secunet sites on these areas were identified, as the office structure results in minimal ecological interactions. Therefore, the ESRS E4 Biodiversity and ecosystems was deemed non-material for secunet.

Furthermore, no significant dependencies of secunet's business activities on biodiversity or ecosystem services were identified. Due to its predominantly office-based activities, there are no direct or indirect operational dependencies on biological resources or ecosystem functions.

The analysis also identified no material physical or transition risks related to biodiversity and ecosystems. Likewise, no material opportunities related to biodiversity and ecosystems were identified.

Systemic risks related to the loss of biodiversity or the degradation of ecosystems were not considered relevant for secunet due to the business model and the low ecological interactions of the sites.

E5

For the report on ESRS E5, secunet's product business was given particular focus. Various stakeholders were involved in an internal exchange, including the unit responsible for product management and development within the CTO office, the Supply Chain Operations and Environmental Management departments, and the product managers.

Governance

G1

As part of our governance standard, the identification of IROs is carried out by the Compliance Office in close coordination with the Sustainability department. In this process, we benefit from the Compliance Office's expertise and its in-depth understanding of our Company.

This assessment is based on insights gained from the daily work of the Compliance Office and company-wide guidelines and regulations. The analysis encompasses the entire company to ensure a consistent strategic direction in the area of governance and to embed our corporate values in all areas.

Environment

ESRS E1 – Climate change

Disclosure requirements in connection with ESRS 2 SBM-3 – Material impacts, risks and opportunities and their interaction with strategy and business model

As an IT security company with a growing infrastructure, we are aware of the importance of using resources responsibly. Increasing digitalization and the rising demand for computing power lead to higher energy consumption, making sustainable solutions and the increased use of renewable energies ever more relevant.

We are actively committed to minimizing our environmental impact. This includes reducing our own energy consumption and adapting to the increasing sustainability requirements of our business partners. At the same time, our IT security solutions help support companies on their path to more climate-friendly digitalization and drive sustainable innovation.

IROs		Position in the value chain			Time horizon		
		Upstream	Own activities	Downstream	Short term	In the medium term	In the long term
Supply chain disruption Natural disasters such as storms, earthquakes, or floods can negatively impact the production or delivery capabilities of suppliers and partners. This, in turn, could affect deliveries and lead to shortages, as global supply security is compromised.	(Physical) Risk		X		X	X	X
GHG emissions Even if greenhouse gas emissions are low, emissions are still generated by business activities.	Actual negative impact	X	X	X	X	X	X
Increasing regulation & rising energy costs Increasing regulation and rising energy costs could lead to higher operating and administrative costs for secunet. Stricter regulations for energy-intensive products further increase the effort required to comply with legal requirements and weaken the company's competitive position. At the same time, rising energy prices are driving production and service costs even higher.	(Transitional) risk	X	X	X		X	
Use and development of energy-efficient solutions Energy consumption through the use of secunet products, both PCs/notebooks and data centers, is decreasing.	Potential positive impact		X	X			X
Customers reject higher prices Customers may not accept higher prices for climate-friendly products, which poses sales risks.	(Transitional) risk			X			X

IROs		Position in the value chain			Time horizon		
		Upstream	Own activities	Downstream	Short term	In the medium term	In the long term
Energy consumption from fossil fuels Energy consumption from fossil fuels causes higher emissions and occurs along the entire value chain – from raw material extraction and production to the operation of secunet sites and the use and return of the products.	Actual negative impact	X	X	X	X	X	X
Climate protection as a source of innovation Sustainable technologies promote innovative business models and increase competitiveness. Furthermore, cost reductions are possible through lower energy consumption.	Opportunity	X	X	X			X

The list of IROs highlights sustainability issues that, if inadequately managed, can negatively impact our business (risks) or have negative consequences for nature and the climate (negative impacts). However, sustainability issues can also bring positive effects – both for the environment and in the form of financial opportunities.

Assessment of resilience based on climate risk analysis

Category	Evaluation
Physical risks	They exist, but are not classified as critical for secunet.
Transition risks	Low, as secunet has proven to be adaptable to regulatory changes.
Overall resilience	secunet is largely resilient to climate risks. Its geographical location in Germany and existing adaptation measures contribute to its stability.
Future steps	Annual review of the analysis to take new developments into account.

Scope: Entire secunet Group; including relevant value chain stages. Exclusions for direct suppliers due to limited data.

Date: Initial analysis 2024, plausibility check July 2025.

Time horizon: 5–25 years, until 2050.

Scenarios:

- Net Zero 2050
- Worst Case (SSP5-RCP8.5)

Methodology: The analysis was based on a qualitative and semi-quantitative scenario assessment involving relevant internal stakeholders (including supply chain operations, purchasing, HR, and facility management). The aim was to systematically identify potential physical and transition risks in the context of different climate scenarios and to assess their impact on the business model.

The analysis made critical assumptions about macroeconomic developments, particularly regarding the increasing internalization of climate costs, rising regulatory requirements, and potential price and demand effects resulting from the transformation to a lower-carbon economy. It was assumed that transition risks could lead to altered cost structures, increased administrative burden, and greater volatility in individual procurement markets in the medium to long term, without, however, significantly impacting the fundamental demand for secunet's digital security solutions.

Regarding energy consumption, it was assumed that the Group's overall energy demand would remain moderate due to its business model. At the same time, a gradual increase in electricity demand was anticipated, particularly due to increasing digitalization, IT infrastructure, and data center services. Efficiency gains from modern building technology, IT optimizations, and organizational measures were considered as a mitigating factor.

Regarding the energy mix, it was assumed that the share of renewable energies in electricity procurement would increase significantly in the long term, driven by regulatory requirements, market availability, and corporate procurement decisions. At the same time, it was assumed that fossil fuels would be associated with rising costs and availability risks in the medium to long term. These developments were taken into account in the assessment of potential transition risks and in the evaluation of long-term cost stability.

In addition, technological developments such as advances in the energy efficiency of IT systems, the increased use of digital solutions, and more resilient supply and operational structures were considered as key influencing factors in the scenarios. Overall, these assumptions contribute to a realistic assessment of the business model's robustness in the face of climate-related transformation processes.

E1-1 Transition plan for climate change mitigation

As a company, we are doing our part to limit global warming to 1.5°C. Therefore, we aim to reduce our emissions to net zero by 2040 and to cut them by 42 percent in Scope 1 & 2 and by 25 percent in Scope 3 by 2030. For Scope 3, this includes purchased goods and services, capital goods, and upstream transport by 2030.

Our transition plan is compatible with the 1.5-degree pathway and the EU target of climate neutrality by 2050. We have no activities or exposures in the coal, oil, or gas sectors.

Our voluntary climate targets meet the highest scientific standards, are aligned with the guidelines of the Science Based Targets initiative (SBTi), and have been successfully validated by SBTi. The target is based on our CO_2 footprint in 2022. Based on this, we have identified decarbonization measures at our sites and along our entire value chain.

To ensure that the set targets are achieved, we have drawn up a transition plan that includes the following actions:

At the sites: replacement of fossil fuels and switch to renewable electricity sources.

Along the value chain: revision of product design and material selection, and integration of suppliers into the sustainability strategy.

Due to secunet's business model, which operates without significant production facilities, the implementation of the transition plan will require minimal capital expenditures (CapEx) or additional operating expenses (OpEx). Instead, achieving the objectives will result from the reallocation of existing resources, for example, by switching from company cars with combustion engines to electric vehicles or by making changes to product design that lead to a lower PCF (Product Carbon Footprint). Currently, expenses consist of planning and initiating projects. These primarily involve personnel costs, which are covered by existing resources. Potentially, CapEx and OpEx may arise, but this cannot be estimated at the time of writing. Currently, there are no objectives or plans to align our taxonomy-eligible economic activities with the criteria set out in Commission Delegated Regulation (EU) 2021/2139 and thus achieve taxonomy conformity.

There are currently no locked-in greenhouse gas emissions associated with our main assets and products. Furthermore, we are not exempt from the EU reference values agreed upon in Paris. The transition plan is integrated into our overall business strategy and has been approved by senior management. The transition plan is aligned with secunet's business model, as evidenced by the fact that the decarbonization levers are based on it. Our business strategy focuses on developing new products and further developing existing ones. These activities are increasingly geared towards emissions reduction.

Decarbonization lever	Action	Time horizon
Replacing fossil fuels	Conversion of company cars to electric cars by 2030	2025 - 2030
Switch to renewable energy sources	Use of electricity from renewable energy sources at all locations by 2026	2022 - 2026
Revision of product design and material selection	Initiative to enhance sustainability features of secunet products	2025 - tba
Integrating suppliers into the sustainability strategy	Increasing transparency regarding Scope 3 emissions across the entire Group by collecting primary data from our A+ suppliers	2025 - tba

E1-2 Policies related to climate change mitigation and adaptation

secunet aims to minimize the negative environmental impacts of its business activities and environmental risks for the company, and to use resources efficiently. This includes, in particular, reducing greenhouse gas emissions and energy consumption wherever feasible and effective options exist.

For this purpose, an environmental management system according to DIN EN ISO 14001 was implemented, with initial certification taking place in September 2024. Key components of the environmental management system include both the environmental policy and the environmental guidelines, which serve as a framework for environmentally responsible conduct and are addressed to all employees. Furthermore, it is ensured that all activities comply with the relevant environmental laws and regulations, and that employees are informed and trained on compliance. The interests of our stakeholders, such as employees and customers, were also taken into account.

The concept for environmental activities is based on the identified material impacts, risks, and opportunities. This includes, in particular, considering transition risks that may arise from changing customer requirements and regulatory requirements in the area of climate protection. Failure to meet future procurement targets could have significant financial consequences. Therefore, secunet pursues a proactive approach to integrate environmental aspects into business development at an early stage and to offer sustainable solutions.

The environmental management system applies to secunet Security Networks AG and encompasses all of the company's locations. The system applies to all activities within the organization and considers its impact on upstream and downstream value chains. The Management Board is responsible for implementing the environmental management system, with coordination carried out by the Environmental Management department in close collaboration with the Sustainability department.

In addition to ISO 14001 certification, the company has committed to upholding the principles of the United Nations Global Compact (UNGC). The interests of key stakeholders were considered through a double materiality assessment, which forms the basis for our environmental activities. This assessment ensures that our environmental activities are aligned with the expectations and concerns of relevant stakeholders.

A key area of focus is reducing energy consumption from fossil fuels in order to lower direct and indirect greenhouse gas emissions. Even though overall emissions are low, they still result from business activities and are to be further minimized through targeted measures. At the same time, secunet is increasingly relying on the use of renewable energies to achieve a positive environmental impact and reduce its dependence on fossil fuels.

Another key issue is adaptation to climate change, particularly with regard to potential supply chain bottlenecks. These risks are regularly assessed and updated to ensure sustainable resilience in procurement processes. Furthermore, any shifts in demand due to changing environmental requirements on the part of customers are actively monitored and taken into account.

The environmental efforts described are made transparent to internal and external stakeholders and kept available via appropriate communication channels to ensure broad acceptance and support.

E1-3 Actions and resources in relation to climate change policies

Meaning and objective

Reducing our climate impact is of high strategic importance to us in the coming years. As outlined in the transformation plan, key actions have already been initiated and further actions are in the planning stages to achieve the targeted emission reductions. Our Company is following a clearly defined roadmap for reducing emissions in Scope 1, Scope 2, and Scope 3.

The ability to implement the described actions is not dependent on the availability or specific allocation of additional financial or other resources. The actions are an integral part of the organization and can be implemented within the existing organizational, personnel, and financial structures.

Replacing fossil fuels

In financial year 2025, a decision was made to comprehensively revise the company car policy in 2026. Starting in 2026, the existing fleet will be gradually converted to fully electric vehicles. The complete conversion is planned for no later than 2030. This will make a significant contribution to reducing direct emissions (Scope 1).

No significant additional investment or operating expenditure (CapEx or OpEx) is required to implement this action, as the changeover will take place within the framework of regular replacement and procurement cycles.

Use of renewable energies

Since financial year 2022, we have covered our electricity needs entirely from renewable energy sources at the vast majority of our locations (99.7%). Conventional electricity is still used at two market locations (0.3%). The conversion of these locations to renewable energy is planned from financial year 2026.

This action will contribute permanently to reducing our site-related emissions (Scope 2) and will be continued.

This action also does not require significant additional CapEx or OpEx expenditures, as it is based on existing energy supply contracts.

Sustainable product design and material selection

We are currently conducting a comprehensive sustainability assessment of our products. This involves analyzing the opportunities for influence within the various life cycle phases in order to identify potential improvements and derive targeted measures for the ecological optimization of our products.

The analyses and the actions derived from them are implemented within the framework of existing development and optimization processes, without requiring significant additional financial resources.

Integrating suppliers into the sustainability strategy

A significant portion of our greenhouse gas emissions originates in the upstream and downstream value chain. Approximately 90% of emissions are attributable to purchased goods, services, and capital goods (Scope 3). Therefore, integrating our suppliers is a key component of our climate strategy.

In 2025, all A+ suppliers were surveyed for the first time regarding the Product Carbon Footprints (PCFs) of the products they supplied to us, as well as their own climate targets. Based on the feedback, adjustments could already be made to the emissions calculations in the "Purchased Goods and Services" category. This close collaboration forms the basis for the continuous decarbonization of the entire value chain.

The implementation of the described supplier measures is carried out without the need for significant additional CapEx or OpEx funds, as it is integrated into existing supplier management and procurement processes.

E1-4 Targets related to climate change mitigation and adaptation

Anchoring the processes

The processes for implementing the requirements of ESRS E1 "Climate change" are firmly established in the relevant departments. They ensure compliance with all relevant legal requirements and the effective implementation of climate-related actions. Furthermore, environmental aspects are continuously considered within the framework of our ISO 14001 certified environmental management system. This system ensures that ecological considerations are systematically integrated into our business processes and continuously improved.

Emission reduction targets and scientific basis

Our emissions reduction targets are based on sound scientific evidence. We have aligned ourselves with the short- and long-term net-zero targets of our main shareholder, which have been validated by the Science Based Targets initiative (SBTi). As part of this process, the base year 2022 was recalculated retrospectively to ensure methodological consistency and comparability.

Our greenhouse gas reduction targets are based on the same system boundaries as our greenhouse gas inventory. Both the inventory and our reduction targets encompass all consolidated companies in accordance with operational control (GHG Protocol).

We commit ourselves to

- to reduce absolute greenhouse gas emissions in Scope 1 and Scope 2 by 42% by 2030 compared to the base year 2022. This target is in line with the 1.5°C target of the 2015 Paris Climate Agreement.
- to reduce absolute greenhouse gas emissions in Scope 3 – from purchased goods and services, capital goods, and upstream transport and distribution – by 25% over the same period. This target contributes to limiting global warming to well below 2°C above pre-industrial levels.

In the long term, we aim to achieve net-zero emissions by 2040. To this end, absolute greenhouse gas emissions in Scope 1, 2, and 3 – including all relevant categories such as purchased goods and services, capital goods, energy-related activities, business travel, and the use and disposal of sold products – are to be reduced by 90% compared to the base year 2022. The remaining 10% will be offset through compensation measures.

Adjustment of the base year

Compared to the previous year's report, the base year was adjusted from 2023 to 2022. This change was made to harmonize our own targets with the science-based climate targets of our main shareholder according to SBTi.

For this purpose, data for the 2022 financial year were collected retrospectively or – where necessary – supplemented based on reliable estimates. Complete emissions data are now available for Scope 1, 2, and all Scope 3 categories classified as significant. Both the Science Based Targets initiative and the Greenhouse Gas Protocol require a base year that representatively reflects typical business activities. The chosen year, 2022, meets this requirement and also represents a meaningful reference year for our company structure.

Overview of targets and progress

The following table summarizes the defined emission targets and the current implementation status. It serves as a central basis for monitoring the success and evaluating the progress of our climate protection measures.

Target	Base year	Value in the base year	Target year	Value in the target	Value in FY 2025	Scenario	Progress
Absolute reduction Scope 1+2*+3 by 90%	2022	106,807 tCO_2e	2040	10,681 tCO_2e	89,169 tCO_2e	1.5°C	18.3%
Absolute reduction Scope 1 + 2* by 42%	2022	637 tCO_2e	2030	370 tCO_2e	671 tCO_2e	1.5°C	-12.7%
Absolute reduction Scope 3 (3.1, 3.2, 3.4) by 25%	2022	97,895 tCO_2e	2030	73,421 tCO_2e	77,967 tCO_2e	significantly below 2°C	81.4%
Procurement of electricity from renewable sources	2022	99.5%	2026	100.0%	99.7%	n/a	99.7%
Conversion of company cars to electric vehicles	2022	453 tCO_2e	2030	240 tCO_2e	448 tCO_2e	n/a	2.3%

* The market-based method is used to calculate the Scope 2 emissions included in the target.

E1-5 Energy consumption and energy mix

	Energy consumption and energy mix		2024	2025
-1	Total consumption of fossil energy	MWh	2,922	2,883
	Share of fossil sources in total energy consumption	%	51.3%	52.9%
-2	Consumption from nuclear power sources	MWh	0	0
	Share of consumption from nuclear sources in total energy consumption	%	0	0
-3	Fuel consumption from renewable sources, including biomass (also industrial and municipal waste of biological origin, biogas, hydrogen from renewable sources, etc.)	MWh	0	0
-4	Consumption from purchased or received electricity, heat, steam and cooling and from renewable sources	MWh	2,774	2,568
-5	Consumption of self-generated renewable energy that is not fuel	MWh	0	0
-6	Total consumption of renewable energy (sum of lines 3 to 5)	MWh	2,774	2,568
	Share of renewable sources in total energy consumption (market-based)	%	48.7%	47.1%
	Total energy consumption (sum of lines 1 and 6)	MWh	**5,697**	**5,451**

Data collection on energy consumption:
secunet's facility management records all relevant building-specific energy consumption data such as electricity, heat, cooling and gas.

Since January 1, 2022, we have primarily sourced our electricity as certified renewable energy from the Krefeld municipal utility company. Currently, 99.7% of our electricity comes from renewable sources.

E1-6 GHG gross emissions

Emissions

		Retrospective				Milestones and target years		
		Base year	Comparison = previous year of N	N		Short-term goal	Long-term goal / net-zero goal	
		2022	2024*	2025	% N / N-1	2030	2040	Annual % of target / base year
Scope 1 greenhouse gas emissions								
Scope 1 GHG gross emissions	(t CO_2e)	474	459	469	2.18	275	0	5.56
Percentage of Scope 1 greenhouse gas emissions from regulated emissions trading systems	(%)	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.
Scope 2 greenhouse gas emissions								
Site-specific Scope 2 GHG gross emissions (t CO_2e)	(t CO_2e)	1,077	1,026	988	-3.70	n/a.	n/a.	n/a.
Market-related Scope 2 GHG gross emissions (t CO_2e)	(t CO_2e)	163	173	203	17.34	95	0	5.56
Significant Scope 3 greenhouse gas emissions								
Total indirect (Scope-3) gross greenhouse gas emissions (t CO_2e)	(t CO_2e)	106,170	105,852	88,497	-16.40	n/a.	10,617	5.56
1 Purchased goods and services	(t CO_2e)	97,493	95,586	75,921	-20.57	71,915	9,589	5.01
2 Capital goods **	(t CO_2e)	n/a.	n/a.	1,607	n/a.	1,205	161	6.67
3 Activities related to fuels and energy (not included in Scope 1 or Scope 2)	(t CO_2e)	192	196	201	2.55	n/a.	19	5.56
4 Upstream transport and distribution	(t CO_2e)	402	1,061	436	-58.91	301	40	5.56
5 Waste generation in businesses	(t CO_2e)	29	10	7	-30.00	n/a.	3	5.56
6 Business trips	(t CO_2e)	414	719	756	5.15	n/a.	41	5.56
7 Commuting employees	(t CO_2e)	1,085	1,394	1,496	7.32	n/a.	109	5.56
8 Upstream leased assets	(t CO_2e)	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.
9 Downstream transport	(t CO_2e)	36	95	39	-58.95	n/a.	4	5.56
10 Processing of sold products	(t CO_2e)	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.
11 Use of sold products	(t CO_2e)	6,306	6,570	7,772	18.30	n/a.	631	5.56
12 Treatment of products at the end of their life cycle	(t CO_2e)	213	222	263	18.47	n/a.	21	6
13 Downstream leased assets	(t CO_2e)	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.
14 Franchises	(t CO_2e)	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.

		Retrospective				Milestones and target years		
		Base year	Comparison = previous year of N	N		Short-term goal	Long-term goal / net-zero goal	
		2022	2024*	2025	% N / N-1	2030	2040	Annual % of target / base year
15 Investments	(t CO_2e)	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.	n/a.
Total GHG emissions								
Total GHG emissions (site-specific)	(t CO_2e)	107,721	107,337	89,954	-16.19	n/a.	n/a.	n/a.
Total GHG emissions (market-related)	(t CO_2e)	106,807	106,485	89,169	-16.26	n/a.	10,681	5.56

* The emission figures for 2024 stated in this document differ from the figures published in the 2024 Annual Report, as more recent invoices have been received and the calculation bases have been updated since then.

** The software used for calculating emissions only enabled separate recording of capital assets from the 2025 financial year onwards.

Determination and estimation of key figures

Estimates are sometimes used to determine the key figures for calculating emissions. The following table shows where in the report – apart from Scope 3 – such estimates are used in the ESRS E1 key figures.

Topic area	Key figure	Basis for calculation	Type of data collection	Estimate (yes/no)	Explanation of the estimate
Energy	Electricity consumption	Consumption in the previous calendar year	Billing data from the previous year	Yes	The previous year's consumption is used as the basis for calculation, as invoices for the reporting year are not yet available.
Energy	Gas consumption	Latest available utility or energy bill	Billing data from the previous year	No	Use of actual billed consumption data
Energy	District heating (partially)	Latest available utility bills	Billing data from the previous year	No	No estimate for locations with reported consumption.
Energy	District heating (partially)	Projection based on number of employees	Plausibility-based projection	Yes	For locations without utility billing, a projection is made based on comparable locations.
Energy	District cooling	Latest available utility or energy bill	Billing data from the previous year	No	Use of actual billed consumption data
Energy	Company car	Liters of fuel or kWh charged in the financial year	Consumption data	No	Data collection based on actual refueling and charging processes
Water	Water consumption (partially)	Latest available utility bills	Billing data from the previous year	No	No estimate for locations with reported consumption.
Water	Water consumption (partially)	Projection based on number of employees	Plausibility-based projection	Yes	For locations without an energy performance certificate, an extrapolation is made based on comparable locations.
Waste	Office waste (landlord-managed disposal)	Estimate	The amount of waste is calculated by multiplying the office space by the average value from an external website.	Yes	Waste quantities are estimated, as no disposal records are available.
Waste	Waste disposal (tenant)	Disposal certificates	Documented quantities	No	Calculation based on actual disposal receipts

secunet reports on emissions according to the categories and methods defined in the GHG Protocol.

The emissions are calculated using specialized software. The emission factors stored therein are based on comprehensive emission factor databases, which are regularly updated with the latest emission factors.

The reported figures refer to the parent company secunet Security Networks AG as well as all subsidiaries.

Scope 1 emissions

The emission factors of the UK Department for Environment, Food and Agriculture (DEFRA) are used to determine Scope 1 emissions.

No biogenic CO_2 emissions from the combustion or biological degradation of biomass occurred during the reporting year; accordingly, such emissions are not included in the disclosed Scope 1 greenhouse gas emissions.

Scope 2 emissions

Scope 2 emissions are calculated using two methods.

- Location-based: Location-based emissions from purchased electricity are calculated using average grid emission factors per location. Contractual instruments cannot be taken into account with the location-based method.
- Market-based: The market-based method takes into account the renewable energy certificates applicable to electricity consumption. The share of certified green electricity is 99.7% of total electricity consumption.

No biogenic CO_2 emissions from the combustion or biological degradation of biomass occurred during the reporting year; accordingly, such emissions are not included in the disclosed Scope 2 greenhouse gas emissions.

Scope 3 emissions

Scope 3 emissions are calculated using different approaches depending on the Scope 3 category.

The calculation of Scope 3 greenhouse gas emissions is based on data from activities within the Group's upstream and downstream value chain.

These categories do not include any indirect Scope 3 greenhouse gas emissions originating from the consolidated accounting group, which includes both the parent company and its subsidiaries.

Scope 3 greenhouse gas emissions from associated companies, joint ventures or non-consolidated subsidiaries are not reported, as secunet has no affiliated companies of this type, with the exception of an inactive subsidiary which is not consolidated due to its non-materiality.

No biogenic CO_2 emissions from the combustion or biological degradation of biomass were generated in the reporting year; accordingly, such emissions are not included in the disclosed Scope 3 greenhouse gas emissions.

The following table provides an overview of Scope 3 metrics for which estimates based on average data or approximations from the upstream and downstream value chain were used, including the respective methodology and assessment of the level of accuracy.

Scope 3 category	Key figure	Proportion of estimated data	Basis for creation / Input sources	Cause of the estimation uncertainty	Estimated degree of accuracy
3.1 Purchased goods and services	Scope 3 emissions (tCO_2e)	Partially (72%)	Combination of spend-based method (purchase volumes × industry-specific emission factors) and supplier-specific method based on supplier-specific emission data	Lack of primary data for a large proportion of suppliers; use of sectoral averages.	Medium
3.2 Capital goods	Scope 3 emissions (tCO_2e)	Mostly	Spend-based method based on investment expenditures and industry-specific emission factors	No object-specific emission data available for individual capital goods.	Medium
3.3 Activities related to fuels and energy	Scope 3 emissions (tCO_2e)	Mostly	Average data method using standardized emission factors	Use of general averages instead of location-specific primary data	Medium
3.4 Upstream transport	Scope 3 emissions (tCO_2e)	Partially	Spend-based method for warehouse transport; route transport not separately quantifiable and included in purchasing costs	Lack of separate cost reporting and activity data for route transport	Medium to low
3.5 Waste volume	Scope 3 emissions (tCO_2e)	Mostly	Average data method using standardized emission factors	Missing primary data specific to quantity and disposal	Medium

Scope 3 category	Key figure	Proportion of estimated data	Basis for creation / Input sources	Cause of the estimation uncertainty	Estimated degree of accuracy
3.6 Business trips	Scope 3 emissions (tCO_2e)	Partially	Activity data (air and train kilometers) combined with average factors; rental car and public transport expenditure-based	Use of flat-rate emission factors for parts of mobility	Medium
3.7 Employee commuting	Scope 3 emissions (tCO_2e)	Complete	Average data method based on external online research on commuting behavior (distances, means of transport)	Assumptions about mobility behavior; no company-specific survey	Low
3.9 Downstream transport	Scope 3 emissions (tCO_2e)	Complete	Derivation based on a flat-rate share (9%) of the emissions from upstream transport (3.4) based on group values	Using an approximate value without using your own activity data	Low
3.11 Use of sold products	Scope 3 emissions (tCO_2e)	Partially	Using Product Carbon Footprints (PCFs) of a representative Lenovo model; extrapolating to total sales	Projection based on a representative product	Medium
3.12 End-of-life treatment of sold products	Scope 3 emissions (tCO_2e)	Partially	Derivation from PCFs focusing on the disposal phase; extrapolation analogous to category 3.11	Use of average disposal assumptions and projections	Medium

Non-relevant Scope 3 emissions

The following Scope 3 categories were deemed not relevant for secunet because they do not occur within the value chain and business model:

- 3.8 Upstream leased assets
- 3.10 Processing of sold products
- 3.13 Downstream leased assets
- 3.14 Franchises
- 3.15 Investments

GHG intensity

Total GHG emissions per net sales revenue		2024	2025	% N/N-1
Net sales revenue	euro	406,400,000.00	458,800,000.00	
Total GHG emissions (site-specific) per net sales revenue	($t\ CO_2e$/euro)	0.000264	0.000196	-25.8%
Total GHG emissions (market-based) per net sales revenue	($t\ CO_2e$/euro)	0.000262	0.000194	-25.9%

The revenue of the secunet Group was calculated according to IFRS.

E1-8 Internal carbon pricing

No internal CO_2 pricing systems are used.

ESRS E5 – Resource use and circular economy

Disclosure requirements in connection with ESRS 2 SBM-3 – Material impacts, risks and opportunities and their interaction with strategy and business model

We rely on highly qualified employees and the essential hardware they use to develop customized solutions for our customers. secunet's business operations are primarily office-based and located in urban areas. In our offices and data centers, we utilize modern, high-performance hardware to ensure efficient business operations.

The materiality assessment identified only the issue of waste as material.

IROs		Position in the value chain			Time horizon		
		Upstream	Own activities	Downstream	Short term	Medium term	Long term
Use of recycled and recyclable packaging Our environmentally friendly packaging solutions rely on recycled and recyclable materials. By reusing the packaging of the original product, we avoid the need for additional packaging.	Actual positive impact	X	X	X	X	X	X

The list of IROs highlights sustainability issues that, if inadequately managed, can negatively impact our business (risks) or have negative consequences for nature and the climate (negative impacts). However, sustainability issues can also bring positive effects – both for the environment and in the form of financial opportunities.

E5-1 Policies related to resource use and circular economy

To date, secunet does not have an official concept for managing its material impacts, risks, and opportunities related to resource use and the circular economy. In fact, these issues are addressed and resolved by complying with the necessary regulatory requirements: currently, only statutory regulations (such as the German Electrical and Electronic Equipment Act (ElektroG), the German Packaging Act (VerpackG), the German Battery Act (BattG), and European EPR, WEEE, BATT, and PACK directives) are adhered to. Product Management and Supply Chain Operations are responsible for implementation.

secunet's business model does not involve its own production facilities. Hardware components are exclusively purchased and resold as bundled products in conjunction with software. Consequently, the design of the upstream value chain is limited. However, considerations and planning regarding resource utilization and the circular economy are possible both within the company and in the downstream value chain.

E5-2 Actions and resources related to resource use and circular economy

Measures related to resource use and the circular economy are not yet comprehensively documented at secunet due to the lack of a corresponding concept. However, some elements in this regard should certainly be mentioned:

- For products in the SINA L3 Box S, SINA L3 Box E/H, SINA Workstation S and SINA Workstation Terminal E/H series, recycled packaging materials are used to reduce packaging waste.
- With SINA Workstation S, secunet enables used laptops to be restored to their original condition at the end of their life cycle ("refurbished") and used for alternative purposes. This is intended to reduce the generation of electronic waste.
- Within the framework of legal requirements, secunet ensures environmentally sound disposal of electronic waste at the end of the product life cycle and makes sure that all EPR (Extended Producer Responsibility) requirements are met.

These actions will be continued on an ongoing basis.

E5-3 Targets related to resource use and circular economy

Since there is no specific concept for resource use and the circular economy, no corresponding targets have been set to date. Setting such targets is not currently planned.

Our established processes are embedded in the relevant departments, which ensure compliance with legal requirements on a daily basis. Environmental issues are also continuously addressed within the framework of our ISO 14001 certifications. The effectiveness of the actions described above is not currently being tracked with regard to the material impacts, risks and opportunities (IROs).

E5-5 Resource outflows

Waste

secunet sells IT products that become electronic waste after their useful life. To ensure the sustainable and responsible handling of this waste, legislators have introduced extended producer responsibility. This obligates manufacturers to organize the disposal, recycling, and environmentally sound treatment of their products. secunet fulfills these requirements by ensuring the take-back and proper disposal of its products, as well as promoting recycling to conserve resources and minimize environmental impact.

Packaging materials are used for shipping; to reduce the resulting packaging waste, secunet uses the packaging material from purchased products for onward shipping to customers.

secunet does not generate any radioactive waste as defined in Article 3(7) of Council Directive 2011/70/Euratom.

Since secunet is a tenant at all locations, the landlords are responsible for the disposal of office waste such as paper/cardboard, mixed municipal waste, and packaging (yellow bin/green dot). secunet provides separate containers for all the aforementioned waste types at each location. The actual amount of waste cannot be determined because the landlords do not provide precise data. Therefore, the amount of waste is calculated by multiplying the square footage of the rented space by an average value obtained from an external website.

Furthermore, waste is generated, which secunet disposes of independently. The exact quantities and waste codes are determined annually based on invoices, and the documentation is archived.

The following table provides an overview of the quantities produced:

in tons	Total	Hazardous	Non-hazardous
Amount of waste generated	1.330,49	3,5	1.326,99
Quantity that is withdrawn from disposal	1.143,66	3,5	1.140,16
Preparation for reuse	0	0	0
Recycling	1.143,66	3,5	1.140,16
Other recovery methods	0	0	0
Quantity intended for disposal	186,82	0	186.82
Incineration	186,82	0	186,82
Deposit	0	0	0
Other types of disposal	0	0	0
Amount of non-recycled waste	186,82	0	186,82
Percentage of non-recycled waste	14,04	0	14,08

This table provides a comparison of the last two financial years:

Waste category	Unit	2024*	2025
Hazardous waste that is not disposed of			
Electronic waste	t	1.87	3.50
Non-hazardous waste destined for disposal			
Mixed municipal waste	t	183.89	186.26
High security (data storage media)	t	0.80	0.57
Wood	t	0.00	0.00
Bulky waste	t	3.50	0.00
Non-hazardous waste that is not subject to disposal			
Construction and demolition waste	t	0.00	1.31
Electronic waste	t	1.08	0.83
Mixed packaging / Commercial	t	2.64	0.00
Paper / Cardboard	t	813.38	815.14
Packaging	t	323.22	322.89

* The discrepancies between the reported quantities in the 2024 report and the actual figures are due to subsequent adjustments to our data, such as changes in employee numbers and area information. Additionally, some waste invoices were re-examined. As a result, the retrospectively adjusted figures differ slightly from the originally reported numbers.

During the data refinement process, it was determined that secunet generates small quantities of hazardous waste, which will be reported separately from the 2025 financial year onwards.

EU Taxonomy

As part of its action plan on financing sustainable growth, the European Union (EU) aims to redirect capital flows into sustainable investments. Against this backdrop, the EU Taxonomy Regulation (Taxonomy Regulation) 2020/852 entered into force in mid-2020, classifying which economic activities in the EU are considered environmentally sustainable.

The EU has now published requirements for sustainable economic activities, as defined in the Taxonomy Regulation, for all six environmental objectives (climate action, adaptation to climate change, sustainable use and protection of water and marine resources, transition to a circular economy, pollution prevention and control, and protection and restoration of biodiversity and ecosystems). The descriptions of economic activities in the delegated acts define which activities are eligible for consideration. These are known as taxonomy-eligible economic activities. Only taxonomy-eligible economic activities can be considered environmentally sustainable, provided they meet certain technical assessment criteria and provide minimum social protection. If an economic activity meets the assessment criteria specified in the delegated acts, it is classified as environmentally sustainable and therefore as taxonomy-compliant.

Delegated Regulation 2022/1214 of 9 March 2022 on nuclear power and natural gas is not applicable.

This analysis includes all fully consolidated group companies with regard to their sales revenues, investment and operating expenses. Further information about the fully consolidated group companies can be found in the annual report.

Analysis of taxonomy capability

In an increasingly interconnected world, secunet combines products and consulting to create resilient digital infrastructures and provide the highest possible level of protection for data, applications, and digital identities. secunet specializes in areas with particularly stringent security requirements, such as eGovernment, eHealth, IIoT, and cloud computing. With secunet's security solutions, companies can meet security standards in their digitalization projects and thus accelerate their digital transformation.

To identify the taxonomy-eligible business activities of the secunet Group, those activities that fit secunet's business model were first identified based on a list of potentially taxonomy-eligible activities. Their significance was then validated using financial key figures. This included both the reported items in the consolidated statement of profit or loss and internal financial key figures.

As a result of the analysis, the economic activities 6.5 "Transportation by motorcycles, passenger cars and light commercial vehicles", 7.7 "Acquisition of and ownership of buildings" and 8.1 "Data processing, hosting and related activities" were classified as eligible for taxonomy. This classification was revalidated in 2025 to ensure that the activities continue to meet current requirements.

EU Taxonomy KPIs from secunet

	Taxonomy-eligible proportion	Non-taxonomy-eligible proportion
Sales volume	3%	97%
Capital expenditures (CapEx)	43%	57%
Operating expenses (OpEx)	1%	99%

Key figures for taxonomy-eligible economic activities

Pursuant to Section 289 (1) of the German Commercial Code (HGB), secunet is obligated to apply the regulations of the Taxonomy Regulation. In accordance with Section 315e (1) HGB, secunet's consolidated financial statements as of December 31, 2025, were prepared in accordance with IFRS. The amounts used to calculate the revenue, capital expenditure (CapEx), and operating expenditure (OpEx) figures are based on the figures reported in the consolidated financial statements. Based on an analysis of business activities, the proportion of taxonomy-eligible revenue/investment (CapEx) and operating expenditure (OpEx) to secunet's respective consolidated figures for the 2025 financial year is disclosed.

Sales revenue:

The revenue reported in the consolidated statement of profit or loss for the 2025 financial year amounts to €458.8 million. This figure forms the denominator under the EU Taxonomy Regulation. The sum of the revenues from the taxonomy-eligible economic activities for the 2025 financial year forms the numerator. The taxonomy-eligible revenues identified in this 2025 financial year can be attributed to the business activities of SysEleven GmbH. SysEleven GmbH operates its own cloud infrastructure and leases it to business customers, supplemented by other cloud services, including the Kubernetes platform MetaKube, as well as consulting and IT services.

Capital expenditure (CapEx):

At secunet, the CapEx metric indicates the proportion of capital expenditures that are either related to a taxonomy-eligible activity (CapEx a), to a plan for expanding taxonomy-eligible activities, enable the conversion of taxonomy-eligible activities into taxonomy-compliant activities (CapEx b), or relate to the acquisition of products and services from a taxonomy-eligible activity (CapEx c). Currently, no such CapEx plan exists, therefore CapEx b is not applicable. Capital expenditures are based on additions to tangible and intangible assets, as well as right-of-use assets from leases (including lease adjustments), during the financial year under review, before depreciation and any revaluations for that financial year, and excluding changes in fair value. This also applies to corresponding additions resulting from business combinations.

The capital expenditure (CapEx) calculated in this way and shown in sections "3. Property, plant and equipment", "4. Intangible assets" and "5. Leasing" of the consolidated financial statements amount to €12.8 million for the reporting year 2025.

The sum of acquisitions that reflect taxonomy-eligible investments forms the numerator of the CapEx metric. This includes investments in data processing activities (8.1. Data processing, hosting, and related activities (Annex I)). Outside its core business, secunet can also potentially contribute to climate protection through its investments in its vehicle fleet (6.5. Transportation by motorcycle, passenger car, and light commercial vehicle (Annex I)) and in buildings (7.7. Acquisition of and ownership of buildings (Annex I)).

Operating expenses (OpEx):

The OpEx metric indicates the proportion of operating expenses associated with taxonomy-eligible activities. This includes operating expenses for assets or processes related to taxonomy-compliant activities, including training and other workforce adjustments, as well as direct non-capitalized costs in the form of research and development (OpEx a). The metric also includes operating expenses that are part of the CapEx plan to expand taxonomy-compliant activities or enable the conversion of taxonomy-eligible activities to taxonomy-compliant activities within a predefined timeframe (OpEx b), as well as the acquisition of products from a taxonomy-eligible activity (OpEx c). To calculate the taxonomy-eligible OpEx share, the financial accounting accounts that reflect the direct, non-capitalized costs for research and development (R&D), building renovation measures, short-term leasing, and maintenance expenses were used to determine the denominator.

The numerator is derived from an analysis of the recorded expenditures, which have been captured in the aforementioned accounts and are related to the assets with regard to their taxonomy eligibility. Of the total operating expenditures, data processing (8.1 "Data processing, hosting and related activities" (Annex I)) can be allocated to the taxonomy-eligible economic activities.

The following economic activities of secunet have been classified as eligible for taxonomy with regard to the environmental goal of climate protection:

Taxonomy-compliant activity	Description of the activity	Assignment at secunet
6.5 Transport by motorcycles, passenger cars and light commercial vehicles	Vehicle fleet	CapEx
7.7. Acquisition of and ownership of buildings	Building	CapEx
8.1 Data processing, hosting and related activities	Cloud infrastructure and cloud services from SysEleven GmbH	Revenue, CapEx, OpEx

Taxonomy conformity analysis

Based on the identified taxonomy-eligible economic activities, secunet conducted a taxonomy alignment analysis. This analysis examined whether the economic activities make a substantial contribution to achieving one or more environmental objectives and do not significantly impair one or more of these objectives. Finally, compliance with minimum social protection standards must be guaranteed. If these requirements are met, an economic activity can be classified as taxonomy-compliant.

In connection with the review, documents were requested from our stakeholders and discussions were held in the context of alignment.

Economic activity 6.5 (Transportation by motorcycles, passenger cars and light commercial vehicles)

The Group undertakes capital expenditures that fall under the definition of CapEx c) (Section 1.1.2.2 of Delegated Regulation 2021/2178). To analyze compliance, various stakeholders, particularly leasing providers, requested documentation to assess the aforementioned criteria. For the 2025 financial year, secunet was not provided with sufficiently detailed information. Therefore, a complete assessment of taxonomy compliance could not be carried out on this basis.

Economic activity 7.7 (Acquisition of and ownership of buildings)

The Group uses leased office properties and thereby incurs capital expenditures that fall under the definition of CapEx c) (section 1.1.2.2 of Delegated Regulation 2021/2178). To analyze compliance, the age of the buildings was first examined – properties completed before December 31, 2020, are classified as non-taxonomy-compliant. The properties used by secunet were either occupied before December 31, 2020, or are older than this date. Therefore, this criterion applies.

Economic activity 8.1 (Data processing, hosting and related activities)

SysEleven GmbH's activities in the areas of data processing, hosting, and related services relate to CapEx a), OpEx a) (sections 1.1.2.2 and 1.1.3.2 of Delegated Regulation 2021/2178) and sales revenue. The technical assessment criteria were not met in the reporting year because, firstly, the refrigerants used in the cooling systems of some data centers (e.g., F-gases) have a global warming potential exceeding the limits stipulated by regulations. Secondly, it could not be verified for the other data centers whether all relevant procedures listed in the latest version of the EU Code of Conduct on the Energy Efficiency of Data Centers or in the CEN-CENELEC document CLC TR50600-99-1 had been implemented – this is another regulatory requirement.

As a result, no economic activity currently meets the criteria, which is why it is not possible report EU taxonomy compliance for the secunet Group in the 2025 financial year.

Share of sales revenue from goods or services related to taxonomy-compliant economic activities - disclosure for 2025

				Criteria for a substantial contribution						DNSH criteria ("no significant impairment")									
Economic activities (1)	Code(s) (2)	Absolute sales revenue (3)	Revenue share (4)	Climate protection (5)	Adaptation to climate change (6)	Water and marine resources (7)	Pollution (8)	Circular economy (9)	Biological diversity and ecosystems (10)	Climate protection (11)	Adaptation to climate change (12)	Water and marine resources (13)	Pollution (14)	Circular economy (15)	Biological diversity and ecosystems (16)	Minimum social standards (17)	Taxonomy-compliant (A.1) or taxonomy-eligible (A.2) revenue share 2024 (18)	Category enabling activity (19)	Category of transitional activity (20)
		Currency	(%)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	Percent	E	T
A TAXONOMICALLY ELIGIBLE ACTIVITY																			
A.1 Ecologically sustainable activity (taxonomy-compliant)																			
Sales revenue for ecologically sustainable activities (taxonomy compliant (A.1))		€0.00	— %																
A.2 Taxonomy-eligible but not ecologically sustainable activities (not taxonomy-compliant)																			
Data processing, hosting and related activities	CCM 8.1	€12,794,008.03	3%	EL	N/EL	N/EL	N/EL	N/EL	N/EL	[redacted]							3 %		T
Sales revenue for taxonomy-eligible but not ecologically sustainable activities (non-taxonomy-compliant activities (A.2))		€12,794,008.03	3%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								3 %		T
Total (A.1 + A.2)		€12,794,008.03	3%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								3 %		T
B. Non-taxonomy-eligible activities																			
Sales revenue for non-taxonomy-eligible activities (B)		€446,040,809.14	97%																
Total (A+B)		**€458,834,817.17 €**	**100%**																

Share of capital expenditure (CapEx) associated with taxonomy-compliant economic activities - disclosure for 2025

				Criteria for a substantial contribution						DNSH criteria ("no significant impairment")									
Economic activities (1)	Code(s) (2)	Absolute CapEx (3)	CapEx share (4)	Climate protection (5)	Adaptation to climate change (6)	Water and marine resources (7)	Pollution (8)	Circular economy (9)	Biological diversity and ecosystems (10)	Climate protection (11)	Adaptation to climate change (12)	Water and marine resources (13)	Pollution (14)	Circular economy (15)	Biological diversity and ecosystems (16)	Minimum social standards (17)	Taxonomy-compliant (A.1) or taxonomy-eligible (A.2) revenue share 2024 (18)	Category enabling activity (19)	Category of transitional activity (20)
		Currency	(%)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	Percent	E	T
A TAXONOMICALLY ELIGIBLE ACTIVITY																			
A.1 Ecologically sustainable activity (taxonomy-compliant)																			
CapEx for ecologically sustainable activity (taxonomy compliant (A.1))		€0.00	— %																
A.2 Taxonomy-eligible but not ecologically sustainable activities (not taxonomy-compliant)																			
Transport by motorcycles, passenger cars and light commercial vehicles	CCM 6.5	€1,612,740.15	15%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								3 %		T
Acquisition of and ownership of buildings	CCM 7.7	€1,209,739.45	11%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								41 %		
Data processing, hosting and related activities	CCM 8.1	€1,977,947.34	18%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								16 %		T
CapEx for taxonomy-eligible but not ecologically sustainable activities (non-taxonomy-compliant activities (A.2))		€4,800,426.94	43%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								60 %		
Total (A.1 + A.2)		€4,800,426.94	43%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								60 %		
B. Non-taxonomy-eligible activities																			
CapEx of non-taxonomy-eligible activities (B)		€6,258,791.98	57%																
Total (A+B)		**€11,059,218.92**	**100%**																

Share of operating expenses (OpEx) associated with taxonomy-compliant economic activities - disclosure for 2025

Economic activities (1)	Code(s) (2)	Absolute OpEx (3)	OpEx share (4)	Criteria for a substantial contribution: Climate protection (5)	Adaptation to climate change (6)	Water and marine resources (7)	Pollution (8)	Circular economy (9)	Biological diversity and ecosystems (10)	DNSH criteria ("no significant impairment"): Climate protection (11)	Adaptation to climate change (12)	Water and marine resources (13)	Pollution (14)	Circular economy (15)	Biological diversity and ecosystems (16)	Minimum social standards (17)	Taxonomy-compliant (A.1) or taxonomy-eligible (A.2) revenue share 2024 (18)	Category enabling activity (19)	Category of transitional activity (20)
		Currency	(%)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J;N; N/EL)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	(J/N)	Percent	E	T
A TAXONOMICALLY ELIGIBLE ACTIVITY																			
A.1 Ecologically sustainable activity (taxonomy-compliant)																			
OpEx for ecologically sustainable activity (taxonomy compliant (A.1))		€0.00	— %																
A.2 Taxonomy-eligible but not ecologically sustainable activities (not taxonomy-compliant)																			
Data processing, hosting and related activities	8.1	€129,007.25	1%	EL	N/EL	N/EL	N/EL	N/EL	N/EL	[redacted]							5 %		T
OpEx for taxonomy-eligible but not ecologically sustainable activities (non-taxonomy-compliant activities (A.2))		€129,007.25	1%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								5 %		T
Total (A.1 + A.2)		€129,007.25	1%	EL	N/EL	N/EL	N/EL	N/EL	N/EL								5 %		T
B. Non-taxonomy-eligible activities																			
OpEx non-taxonomy-eligible activities (B)		€9,568,344.14	99%																
Total (A+B)		**€9,697,351.39**	**100%**																

Activities in the fields of nuclear energy and fossil gas

Line	Activities in the field of nuclear energy	
1	The company is active in the field of research, development, demonstration and deployment of innovative power generation plants that generate energy from nuclear processes with minimal waste from the fuel cycle, finances such activities or holds risk positions related to these activities.	NO
2	The company is involved in the construction and safe operation of new nuclear facilities for the generation of electricity or process heat — including for district heating or industrial processes such as hydrogen production — as well as in improving their safety using the best available technologies, finances such activities or holds risk positions related to these activities.	NO
3	The company is active in the safe operation of existing nuclear facilities for the generation of electricity or process heat — including for district heating or industrial processes such as hydrogen production — as well as in their safety improvement, finances such activities or holds risk positions in connection with these activities.	NO
	Activities in the field of fossil gas	
4	The company is involved in the construction or operation of facilities for generating electricity from fossil gaseous fuels, finances such activities, or holds risk positions related to these activities.	NO
5	The company is involved in the construction, modernization and operation of combined heat and power/cooling plants using fossil gaseous fuels, finances such activities or holds risk positions related to these activities.	NO
6	The company is involved in the construction, modernization and operation of plants for heat generation that produce heat/cold from fossil gaseous fuels, finances such activities or holds risk positions related to these activities.	NO

Social

ESRS S1 – Own workforce

Disclosure requirements in connection with ESRS 2 SBM-3 – Material impacts, risks and opportunities and their interaction with strategy and business model

Our employees are at the heart of our company. We are committed to their personal and professional development and foster an inclusive corporate culture that is based on appreciation and support for all employees. Regardless of gender, age, or location, all employees should have equal opportunities for development.

Our employees may be affected to varying degrees by the impact of our business activities - as shown in the IRO table.

As part of ESRS S1, we have identified the following key matters, among others: data protection, working time arrangements and work-life balance, gender equality, and social dialogue. Our commitment also includes measures against violence and harassment to ensure a safe and supportive working environment.

Furthermore, we invest strategically in training and skills development to offer long-term benefits to both our employees and society. The health and safety of our employees is our highest priority, which is why we continuously improve our health management program. We are also actively committed to the prevention of forced and child labor.

IROs

Sub-sub-matters			Position in the value chain			Time horizon		
			Upstream	Own activities	Downstream	Short term	Medium term	Long term
Working hours	**Limitation of overtime** secunet contractually limits the overtime hours of its employees in order to prevent a culture of excessive overtime. To avoid overtime and prevent overload.	Actual positive impact		X		X		
Working hours	**Missing time tracking** A lack of time tracking can lead to hidden overtime and thus to employee overload. This can negatively impact their health and performance, which in turn can lead to absences or a decline in quality – with potential consequences for secunet's financial performance.	Risk		X			X	
Social Dialogue	**Employee satisfaction** secunet already actively promotes employee satisfaction through involvement in decision-making processes and collaboration with employee representatives. Continuous measures can further strengthen this satisfaction and employee retention.	Actual positive impact		X		X	X	X
Work-life balance; Health & safety	**Increase in attractiveness** Further measures to promote social standards can increase secunet's attractiveness as an employer.	Opportunity		X		X	X	X

Sub-sub-matters			Position in the value chain			Time horizon		
			Upstream	Own activities	Downstream	Short term	Medium term	Long term
Social Dialogue	**Consideration of the needs and wishes of employees** Considering the needs and wishes of employees can increase productivity and reduce the turnover rate. This offers the company opportunities by both increasing efficiency and reducing recruitment costs.	Opportunity		X		X	X	X
Work-life balance	**Flexibility in working hours and location** Flexible working hours based on trust, as well as the option of mobile working and shared desks, allow secunet employees to individually adapt their working hours and location. This promotes a better work-life balance.	Actual positive impact		X		X	X	
Health & Safety	**Promoting employee health** Implementing further measures in the area of health management, e.g. focusing on mental health, can enhance the positive effects on the health of employees.	Actual positive impact		X			X	X
Gender equality	**Promoting women in the IT industry** The IT industry is considered male-dominated. secunet has the opportunity to promote women in the industry and thereby attract competent female employees.	Opportunity		X			X	X
Further education and skills development	**Promoting skills within the workforce** The skills of secunet employees are further developed through training and education.	Actual positive impact		X		X	X	X
Measures against violence and harassment	**Thorough hiring process** In the hiring process, in addition to professional competence, strong emphasis is placed on interpersonal skills. This fosters a positive company culture and collaboration within the company.	Actual positive impact		X		X		

The list of IROs highlights sustainability issues that, if inadequately managed, could lead to adverse effects for individuals (negative impacts) or risks for our company. However, impacts can also be positive, and sustainability issues can potentially bring positive financial effects (opportunities).

S1-1 Policies related to own workforce

secunet pursues various approaches to ensure responsible treatment of its workforce and to systematically manage the impacts, risks, and opportunities associated with our employees. These approaches include human rights commitments, policies for labor and employment practices, and measures to promote health, safety, diversity, and equal opportunities. Responsibility for implementation lies at the highest management level. The policies described in this section apply company-wide.

Work-life balance

As part of our holistic HR strategy, work-life balance is a key component of our HR policy. secunet has held the "berufundfamilie" (work and family) certificate since 2025, which promotes a family- and life-phase-oriented HR policy and contributes to increased job satisfaction, employee retention, and performance. secunet's long-term goal is to further strengthen work-life balance and successfully complete the "berufundfamilie" re-audit by 2028. Currently, secunet is working to further professionalize the underlying structures and strategically expand its family-friendly HR policy.

The scope of application applies company-wide and includes all employee groups. As part of the audit, existing measures – such as flexible working hours, mobile working, counseling and support services, life-phase-oriented personnel development, and health-related benefits – were systematically evaluated and further developed. The targets and measures defined in the audit are regularly monitored and updated. The "work and family" audit thus makes a significant contribution to managing our social impact, opportunities, and risks.

Commitment to international human rights standards

With its declaration of principles on respecting human rights, secunet commits to upholding internationally recognized human rights and the associated human rights and environmental due diligence obligations. We see it as our responsibility to ensure compliance with these standards in our business operations and supply chains and to take measures to prevent human rights violations. Our actions are guided by the principles of the United Nations Universal Declaration of Human Rights, the UN Guiding Principles on Business and Human Rights, the OECD Guidelines for Multinational Enterprises, the Fundamental Principles of the International Labour Organization (ILO), the ten principles of the UN Global Compact (UNGC), and other relevant international agreements. These commitments form the basis of our business practices and our corporate culture. Furthermore, secunet actively promotes diversity, inclusion, and equal opportunities and does not tolerate any form of discrimination based on legally protected characteristics. By signing the Diversity Charter, we have enshrined this commitment in our corporate policy.

Code of conduct as a binding framework

To ensure high ethical standards, our Group-wide Code of Conduct for Employees, updated in 2025, contains binding guidelines on compliance, human rights, and responsible conduct. It includes, among other things, clear regulations against human trafficking, forced labor, and child labor, and refers to adherence to all relevant international standards. Internal reporting channels, control mechanisms, and sanction procedures are in place for the implementation of the Code. Further information on the Code of Conduct can be found in Chapter ESRS G1 - Business Conduct.

Occupational health and safety

Ensuring occupational health and safety is another essential aspect of our responsibility towards our employees. Since 2025, occupational health and safety has been part of the HR department, for which a new position was created. We operate a systematic occupational safety management system that meets all legal and industry-specific requirements and continuously develop measures to promote the physical and mental health of our employees.

S1-2 Processes for engaging with own workforce and workers' representatives about impacts

secunet strives to be an attractive employer and to maintain this attractiveness in the long term. To meet this goal, the company, under the leadership of its HR department, is implementing processes for employee engagement. A key component is continuous dialogue with employees – both individually and at the company level.

Employee surveys as an important feedback tool

To measure employee satisfaction and actively involve them in shaping working conditions, secunet regularly conducts employee surveys. Two surveys were already carried out in 2021 and 2023, which generated considerable interest – the participation rate for the last survey was 72%. The current employee survey started in November 2025; the participation rate was 73.3%. Analysis, communication of the results, and the resulting measures will take place next year.

Based on the 2023 survey, several projects were initiated to improve working conditions and collaboration. These include, in particular, optimizing interdisciplinary collaboration, improving administrative processes – for example, through the planned introduction of a new travel expense tool in 2026 – and increasing the visibility and accessibility of the Management Board.

We are continuing to actively work on the relevant topics from the 2023 survey. We are driving the optimization of interdisciplinary collaboration through the targeted expansion of workshops, exchange formats, and employee events to strengthen cohesion among all employees and promote dialogue between departments. One example of this is the newly introduced onboarding event for all new employees.

The continuous improvement of administrative processes will also continue – including the planned introduction of a Learning Management System in 2026 and the further expansion of Employee Self Service (ESS). In addition, the visibility of the Management Board will be further strengthened through regular meetings and Q&A sessions.

Direct involvement of the workforce

secunet fosters continuous dialogue with its employees to actively incorporate their opinions and concerns into business decisions. Regular dialogue formats, exchanges with managers and the board, and structured feedback mechanisms such as annual performance reviews and goal-setting meetings ensure that employee perspectives and concerns are taken into account.

Furthermore, a works council was established at our subsidiary SysEleven in 2024. This council exclusively represents the interests of SysEleven's employees and strengthens co-determination as well as structured dialogue between the workforce and management.

In addition, the SET Open Floor, a new, regularly held dialogue format, was established to facilitate open and direct exchange between employees and the secunet Executive Team (SET). Members of the entire SET, in rotating groups, meet with employees at various locations without a fixed agenda. The focus is on an informal, personal dialogue where questions, ideas, and topics can be openly raised.

A key instrument for systematically collecting feedback is the secunet employee survey, which is conducted every two years. It provides structured insights into perceptions of work, leadership, communication, company culture, and development opportunities. The results form the basis for transparent dialogues and targeted improvement measures at both the company and team levels, and support data-driven decisions for the further development of the work culture.

The ongoing feedback process ensures that employee interests are incorporated into corporate decision-making. This aims not only to strengthen employee dialogue but also to secure a sustainable and attractive work culture.

S1-3 Processes to remediate negative impacts and channels for own workers to raise concerns

Managers are obligated to report any known or observed incidents. Several channels are available for this: reports can be made directly to the HR department, the Compliance Office, or via the global whistleblower system, which guarantees confidentiality and protection.[4]

We ensure that all employees are informed about the available complaint mechanisms – both during the onboarding process and through internal communication channels. Every report received is treated confidentially.

We consider the channels through which employees can communicate their concerns and needs to be effective, as they are well-established and familiar to employees. Regular dialogues with managers and employee surveys follow a clear schedule. This ensures that measures to improve employee well-being are continuously reviewed and that employee interests are always taken into account.

[4] For more information on the whistleblower system, see G1-1.

S1-4 Actions[5]

Promoting a feedback culture and staff development

secunet places great emphasis on a strong feedback culture to enable in-depth feedback on individual performance. A key component is the annual employee review, which serves as a standardized, structured dialogue between employees and managers. In addition to performance evaluation, aspects such as job satisfaction, workload, and individual development are discussed. This leads to the identification of training needs, resulting in the continuous expansion of the training program. Since 2025, this process has been further supported by a newly created personnel development position that systematically analyzes and addresses development needs.

To meet the demands of the IT sector, secunet focuses on targeted talent acquisition and development. Through university partnerships, internships, thesis projects, and the Germany Scholarship program, secunet secures qualified talent early on. The company is also actively involved in vocational training and offers a trainee program for graduates. In addition, transparent career and development paths are available, providing employees with clear guidance on potential career paths and development steps.

The in-house training program includes IT courses, project management certifications, and programs for personal and methodological skills development. In addition, there are external training courses, coaching sessions, and customized professional development programs tailored to the individual needs of employees. The new HR development unit serves as a central point of contact for the strategic development of these programs and for increasing transparency in the development process.

We manage data and feedback in accordance with our privacy policy and prioritize the well-being of our employees – in line with ethical standards and legal requirements. Employee data is treated with strict confidentiality to facilitate open and constructive feedback through various channels. This approach ensures that our employees feel supported, valued, and included.

Health management and occupational safety

secunet pursues a comprehensive occupational health and safety management system that involves all employees and is continuously developed. Since 2025, occupational safety has been integrated into the HR department to holistically manage health protection, prevention, and systematic health management. A new position was created for this purpose. Its responsibilities include not only overseeing occupational safety but also analyzing and documenting workplace accidents, accident log entries, and accident reports, as well as organizing health days, preventive medical checkups, and relevant training sessions. Based on this, a structured occupational health and safety management concept is developed.

Occupational health services remain a central component of the offering – from preventative check-ups and health consultations to vaccination programs such as regular flu shots at major locations. In addition, secunet promotes both the physical and mental health of its employees through ergonomic workplace design. Regular analysis of workplace accidents and sick leave continues to serve as a tool for identifying areas for improvement.

Since 2025, a company reintegration management program (BEM) has also been in place. Its goal is to maintain the ability to work in the long term, overcome existing periods of incapacity for work, and prevent future periods of sick leave. At the same time, BEM helps to avoid permanent health limitations or chronic illnesses and to ensure continued employment. The BEM officer works closely with the company's medical service to support successful reintegration.

In addition, secunet is continuously expanding its health-promoting offerings, including location-specific sports and exercise programs.

[5] Unless otherwise stated, all measures mentioned in this section are ongoing and valid for the entire group.

Reconciling family and career

In its corporate culture and the promotion of work-life balance, secunet relies on binding standards and flexible frameworks. By signing the Diversity Charter and obtaining the "berufundfamilie" certification, the company commits to a life-phase-oriented personnel policy. Flexible working hours and part-time models, including employment opportunities for people with disabilities, as well as support services through the PME Family Service, contribute to enabling all employees to participate equitably.

Furthermore, promoting work-life balance encompasses various measures, such as the option of mobile working, the use of shared desk models, and remote work from EU countries. In addition, a wide range of advisory services are available – including life coaching and childcare solutions for dependent relatives – as well as additional support measures such as paid special leave or financial assistance for family events. Employees also benefit from perks like bike leasing, public transport passes, and dog-friendly workplaces, which noticeably ease their daily lives.

Diversity, equal opportunities and inclusion

Diversity, equal opportunities, and inclusion are key success factors for secunet's future-oriented corporate culture. Different perspectives foster creativity and innovation, strengthen competitiveness, and contribute to a better understanding of global markets. At the same time, they increase the company's attractiveness as an employer and support long-term employee retention.

secunet is explicitly committed to upholding the principles of equal treatment and rejects all forms of discrimination – regardless of origin, gender, religion, disability, age, or other personal characteristics. This commitment is enshrined in the code of conduct and actively practiced within the company culture.

Ethical corporate governance and reporting channels

secunet is committed to responsible corporate governance, which is complemented by transparent reporting and control mechanisms. All employees, as well as management and supervisory bodies, are bound by the secunet Code of Conduct. Violations can be reported confidentially via internal reporting channels.

Furthermore, compliance with human rights and environmental due diligence obligations is ensured in accordance with the German Supply Chain Due Diligence Act (LkSG). An annual risk analysis reviews potential human rights and environmental risks. The effectiveness of these measures and initiatives is continuously monitored and evaluated by the Compliance department.[6]

We do not report on further measures that serve solely to comply with existing legal requirements and recognized human rights standards. Although we are clearly committed to fair and safe working conditions, reporting on these would merely reflect our compliance with existing regulations and would not indicate a specifically identified impact. Our focus is on maintaining high workplace standards that meet both legal requirements and ethical guidelines – with the aim of ensuring that all employees are treated fairly and respectfully. The effectiveness of HR measures is also monitored through employee surveys.

[6] More information on the effectiveness of these measures can be found in section S2.

S1-5 Targets[7]

Target in the area of further education

secunet's long-term goal is to maintain a consistently high level of employee satisfaction in the area of professional development. This is based on the strategic expansion and professionalization of training programs. A key component is the implementation of a Learning Management System (LMS), which enables the systematic management, evaluation, and allocation of training measures.

Following the successful onboarding of the tool, the company is now in the technical and organizational setup phase. The ongoing operation, the collection of relevant key performance indicators (KPIs), and the development of suitable KPIs are expected to be completed by 2026.

The HR department is responsible for implementation. Key actions include the gradual expansion of targeted training programs and ensuring that the offerings meet the needs and expectations of employees. With these measures, secunet supports the long-term development of skills within its workforce and simultaneously strengthens employee satisfaction and retention.

Target in the area of workplace health management

secunet pursues the long-term goal of ensuring the sustainable health of all employees and continuously expanding occupational health and safety with a focus on prevention. Both physical and mental aspects are central to its workplace health management.

The operational objective includes strengthening preventative health measures and continuously developing health-promoting structures. Responsibility lies with the HR department, specifically the safety and health officer.

Key actions include conducting a psychological risk assessment in 2025 (with results available in early 2026), comprehensive health promotion programs in cooperation with the company's occupational health service – including vaccinations and medical check-ups – and the already completed evaluation of sports facilities. Furthermore, secunet plans to further develop healthy and ergonomic work environments from 2026 onwards to systematically establish long-term occupational health and safety measures.

These measures strengthen prevention, promote well-being and safety, and support employees in a healthy, low-stress working environment.

Target in the area of diversity

secunet is committed to promoting diversity and increasing the proportion of women, particularly in technical roles and management positions. However, a specific, quantitative corporate target has not yet been set.

The proportion of women in relevant employee groups is currently being systematically collected and analyzed. This is based on current data on the employee structure as well as internal personnel statistics. The aim of this data collection is to create a valid basis for defining a company-wide target value.

The next step involves formulating and formally adopting a strategic goal for increasing the proportion of women, based on the findings. The HR department, managers, and relevant specialist departments will be involved in this process.

[7] Since the company's overarching ESG strategy is constantly evolving, no quantitative targets have yet been defined for individual HR aspects. As the ESG strategy matures, quantitative targets will be developed and implemented gradually.

S1-6 Characteristics of the undertaking's employees

Number of employees and gender percentage

Gender	Number of employees (headcount) 2024	Number of employees (headcount) 2025
Women	299	319
Men	932	983
Diverse	0	0
Not specified	0	0
Overall result	**1231**	**1302**

Employee characteristics

	Training contract		Unlimited		Temporary		Overall result	
Gender	2024	2025	2024	2025	2024	2025	2024	2025
Women	4	2	261	285	34	32	299	319
Men	3	2	833	890	96	91	932	983
Diverse	0	0	0	0	0	0	0	0
Not specified	0	0	0	0	0	0	0	0
Overall result	**7**	**4**	**1,094**	**1,175**	**130**	**123**	**1,231**	**1,302**

Method

The total number of employees in the secunet Group is calculated by summing the number of employees at all locations, including those not on paid leave, parental leave, or unpaid leave, excluding the Management Board and freelancers. This calculation is based on the reference date of December 31, 2025. The contract types are defined as follows:

Employees with a training contract

These employees are completing vocational training in which they acquire both theoretical and practical knowledge in their field. During the contractually agreed training period, they are specifically prepared for their future professional activities. This also includes individuals in a dual training program who acquire their theoretical knowledge at a vocational school and gain practical experience in the company.

Employees with a permanent contract

These employees have permanent contracts with the company, contribute to the long-term stability and development of the company, and benefit from continuous professional development.

Employees with a temporary contract

These employees work for the company on a temporary basis, either to cover a temporary need or for project-related tasks. Their involvement offers the company flexibility, while they contribute their skills and expertise for the agreed duration.

Employee turnover

	2024	2025
Departures:	132	133
Additions:	188	204
Headcount as of January 1st of the year	1,187	1,219
Fluctuation in %	**9.6%**	**9.3%**

Method

The employee turnover rate was calculated using the headcount (excluding the Management Board) and the Schlüter formula. All departures were included in the calculation.

S1-8 – Collective bargaining coverage and social dialogue

Currently, there is no institutionalized social dialogue and no collective bargaining agreement covering this issue. Social dialogue takes place through the measures described in sections 1-2. The relevance of this topic will be reviewed next year and adjusted as needed.

S1-9 Diversity parameters

Gender ratio in management

	2024	2025
Number of managers reporting to the Management Board, including subsidiaries	24	30
Of which female	4 (16.7%)	6 (20%)

Method

The management level consists of managers who report directly to the Management Board. This definition corresponds to our company-specific interpretation of top management, as it reflects our business structure and internal reporting lines.

Distribution of employees by age group

	30 - 50		older than 50		under 30		Overall result	
Gender	2024	2025	2024	2025	2024	2025	2024	2025
Women	178	198	52	57	69	64	299	319
Men	535	585	234	242	163	156	932	983
Overall result	**713**	**783**	**286**	**299**	**232**	**220**	**1,231**	**1,302**

Method

The age distribution of employees is determined by summarizing the total number of employees under 30 years of age (29 or younger), between 30 and 50 years of age (30 to 49), and 50 years of age and older. Freelancers and external contractors are not included.

S1-14 Parameters for health protection and safety

Work-related injuries are rare at our workplace because our activities do not place a high physical strain on employees. All employees are covered by our health and safety management system.

	2024	2025
Percentage of employees who are covered by the health and safety management system.	100.0%	100.0%
Number of deaths resulting from work-related injuries and work-related illnesses	0	1
Number and rate of reportable workplace accidents	Accidents: 2 Rate: 0.9246	Accidents: 4 Rate: 2.0327
Number of notifiable work-related illnesses	0	0
Number of days lost due to work-related injuries, illnesses and deaths	37 days	170 days

Method

The figures are collected through employee reports. The rate of reportable workplace accidents was calculated according to the ESRS S1-14 AR. 89 guidelines.

S1-16 Compensation indicators

Gender pay gap

The gender pay gap in the IT industry is heavily influenced by historical factors. More men still complete STEM educations and thus constitute the majority of the talent pool – a fact reflected in leadership positions and the overall company structure. Through targeted diversity initiatives, we strive to balance the gender distribution in leadership positions and throughout the company, ensuring equal pay for equal qualifications and comparable work. Although we pay equal wages for equal work, the industry's gender imbalance impacts the overall statistics. Without these industry-specific factors, our compensation structure would reflect fair remuneration.

At secunet, women earn on average **79.40%** of the salary of their male colleagues, which corresponds to a gender pay gap of **20.60%**. This means that, across all employees, women earn an average of 20.60% less than men. Compared to 2024, the gender pay gap has thus **decreased by 2.59 percentage points**.

However, a detailed analysis of gross salaries shows that this difference is largely influenced by the following factors:

- Occupational groups
- Company affiliation
- Relevant professional experience

Male employees, on average, have been with the company longer and therefore often possess more professional experience. Furthermore, men are currently significantly overrepresented in technical professions such as IT security compared to women. However, an increase in female students is already observable at universities, which is expected to lead to more female applicants in the coming years. This trend could contribute to reducing the gender pay gap in the long term by encouraging more women to enter technical professions and aspire to leadership positions.

Method

The calculation of the gender pay gap at secunet is based on the average annual salary, which is determined as the mean of the annual salaries and leveled to a weekly working time of 38.5 hours, also including working students in the calculation.

Ratio of total remuneration

	Average annual salary leveled to 38.5 hours.		Average annual salary leveled to 38.5 hours.	
	2024	2025	2024	2025
Median	€72,774.04	€75,444.50	€76,588.48	€79,638.00
Highest-ranking individual (Management Board)	€474,999.92	€474,999.92	€474,999.92	€474,999.92
	653.0%	**630.0%**	**620.0%**	**596.0%**
	With temporary workers, trainees, students, etc...		without trainees, students, etc...	

Method

The annual salary is standardized based on a 38.5-hour work week and also includes hourly employees, such as student trainees. For all employees, with the exception of student trainees, the annual salary consists of a fixed monthly gross salary and a variable bonus component. In addition, the highest-earning individual among all employees, including the Management Board, is recorded.

S1-17 Incidents, complaints and severe human rights impacts

Discrimination cases:	2024	2025
a) Total number of discrimination cases	0	0
b) Number of complaints reported via the whistleblower system/ complaint procedure	1	0
c) Total amount of sanctions	0	0

We investigate all reported cases of discrimination and complaints within our company through official channels. Due to the sensitive nature of these issues, we do not disclose details of individual incidents. Every report is treated with the utmost confidentiality. Our grievance mechanisms ensure that employees can report incidents safely and confidentially. In 2025, no fines, sanctions, or compensation payments related to discrimination were recorded.

During the reporting year, we became aware of no serious human rights violations. No fines, sanctions, or compensation payments were recorded in this context.

ESRS S2 – Workers in the value chain

Disclosure requirements in connection with ESRS 2 SBM-3 – Material impacts, risks and opportunities and their interaction with strategy and business model

IROs

Sub-sub-matters			Position in the value chain			Time horizon		
			Upstream	Own activities	Downstream	Short term	Medium term	Long term
Forced labor	**Reputational damage** Potential child or forced labor at secunet's suppliers poses a risk of reputational damage, especially if it becomes public, and can have a negative impact on sales and order intake.	risk	X				X	

The list of IROs encompasses sustainability issues that, if inadequately managed, can pose risks to our company. However, in addition to these potential negative consequences, sustainability aspects can also have positive effects – both socially and through the economic opportunities that arise from a sustainable corporate strategy.

As part of its materiality analysis, secunet identified no material positive or negative impacts on specific groups of workers in the value chain for the 2025 financial year. The risk analysis pursuant to Section 5 of the LkSG (German Supply Chain Due Diligence Act) revealed no evidence of child or forced labor at direct suppliers. Likewise, no particularly vulnerable employee groups were identified; no complaints from indirect suppliers were received during the reporting period.

Despite this seemingly unremarkable starting point, secunet recognizes a material risk in potential violations of social standards by suppliers, particularly regarding working hours, occupational safety, and fair wages. As a provider of security-critical IT solutions with a focus on public procurement, secunet relies heavily on trust, integrity, and legally compliant conduct within its supply chain. Publicly disclosed abuses could lead to reputational damage, exclusion from tendering processes, and significant losses in revenue and EBIT. It could also negatively impact secunet's attractiveness as an employer.

Since secunet does not operate its own physical production facilities but sources specialized hardware and software components from external partners, there is a structural dependency on their labor and social standards. This can lead to minimum standards not being met in parts of the upstream value chain – especially under high time and cost pressures.

To counteract this risk, secunet has established a published policy statement on respecting human rights and a binding supplier code of conduct. Both policies define clear expectations regarding minimum social standards and form the basis for responsible cooperation with suppliers and business partners.

S2-1 Policies related to value chain workers

As a highly specialized IT security company with predominantly technology-based supplier relationships, our value chain consists primarily of suppliers of services, software licenses, and hardware components, most of whom are located within the Eurozone. Therefore, we have only limited influence on the upstream and downstream supply chain. However, we work closely with our most strategically important direct suppliers (Tier 1).

Declaration of principle

This policy statement applies to the entire secunet Group, including all subsidiaries. It covers the company's own business operations as well as the entire supply chain, with the aim of identifying and minimizing human rights and environmental risks and preventing violations of human rights and environmental obligations.[8]

The policy statement is publicly available and has also been communicated internally to employees. It was last updated in April 2025.

The Management Board bears overall responsibility for compliance with and implementation of human rights and environmental due diligence obligations and ensures that these are integrated into the company's strategy and risk management. The Human Rights Officer is responsible for implementing the policy statement and the human rights strategy.

secunet adheres to recognized international standards such as:

- UN Guiding Principles on Business and Human Rights (UNGP)
- Universal Declaration of Human Rights of the United Nations
- OECD Guidelines for Multinational Enterprises
- Core Labour Standards of the International Labour Organization (ILO)
- Ten principles of the UN Global Compact (UNGC)
- Stockholm Convention on Persistent Organic Pollutants (POPs Convention)

The policy statement establishes binding ethical, social, and environmental standards for secunet and its value chain, describes its human rights strategy, and is based on the aforementioned international frameworks. It outlines clear responsibilities at the management level, mechanisms for risk minimization and compliance monitoring, and measures for stakeholder engagement, including a whistleblower system to ensure transparency and continuous improvement.

During the reporting year, secunet recorded no cases of non-compliance with the aforementioned principles and standards.

Code of conduct for suppliers and business partners

secunet explicitly opposes human trafficking, forced labor, and child labor in its own business operations as well as in its upstream and downstream supply chains. These principles are enshrined in the Code of Conduct for Employees, the Code of Conduct for Suppliers and Business Partners, and the company's Policy Statement.[9]

The Code of Conduct for Suppliers and Business Partners is a central element of the L-CMS and is binding for all suppliers and business partners. It was adopted by the Management Board in 2022 and is intended to promote the sustainable development of our supply chain. The Code of Conduct for Suppliers and Business Partners contains clear guidelines that enable us to cooperate responsibly, with integrity, and ethically in accordance with legal regulations.

[8] Unless otherwise stated, all measures mentioned in this section are ongoing.
[9] For more information on the code of conduct, see ESRS G1-1.

The contents of the code are based on the ten principles of the UN Global Compact, the ILO principles and the LkSG.

The code of conduct for suppliers and business partners was developed by the Corporate Compliance department based on the requirements of the LkSG. The interests of employees in the value chain were taken into account.

To ensure compliance with the regulations, audit and information rights are enshrined in secunet's General Terms and Conditions (GTC) and Purchasing Terms and Conditions. The code is available in German and English on the intranet and corporate website.

S2-2 Procedures for engaging with value chain workers about impacts

The double materiality assessment identified no material impacts on workers in the value chain. Therefore, implementing a specific procedure for working with workers in the value chain is not currently necessary. Furthermore, the risk analysis conducted in accordance with the LkSG revealed no material human rights or environmental risks in the supply chain. secunet will review the risk analysis periodically and reassess the need for such a procedure should circumstances change.

S2-3 Processes to remediate negative impacts and channels for value chain workers to raise concerns

Complaint procedure

In addition to its whistleblower system, secunet has established a complaints procedure that offers both internal and external stakeholders, including employees in the value chain, the opportunity to raise human rights and environmental concerns. Complaints can be submitted through various channels:

- Electronic whistleblower system
- E-mail
- Phone
- Letter
- Personal meeting with the human rights officer/compliance officer

The complaints procedure is accessible to internal and external stakeholders via the intranet and the corporate website and is integrated into the compliance guidelines and the secunet codes of conduct.

Should secunet become aware of a lack of access to the complaint procedure at suppliers, appropriate procedures or additional reporting channels will be introduced to enable the affected employees to access the complaint procedure.

The complaints procedure is based on the provisions of the LkSG and ensures a fair, transparent, and effective process. Internal procedures are defined in the "Procedural Guidelines for Whistleblower and Complaint Procedures," which have been published both internally on the intranet and externally on the corporate website.

The procedural guidelines ensure that all reports and complaints are processed objectively and in accordance with procedural principles. In accordance with the German Supply Chain Due Diligence Act (LkSG) and the Whistleblower Protection Act (HinSchG), fixed deadlines for processing have been defined to ensure a swift and structured investigation.

In addition, internal and external stakeholders have the opportunity to communicate via the intranet and the corporate website.

- the processing procedure and the responsible contact persons,
- the protection mechanisms for whistleblowers,
- the functionality of the electronic whistleblower system and
- to provide information on the reporting criteria and the available reporting channels.

No complaints were filed by employees in the value chain regarding the grievance procedure during the reporting year. The effectiveness of the procedure is therefore currently assessed solely on the basis of the framework conditions described.

If a complaint is received via the whistleblower system, we have been sending the complainant a series of targeted feedback questions since August 2025. This allows us to ensure that the whistleblower system and the handling of reported information/complaints meet the needs of the complainants and, if necessary, to identify areas for improvement. Since this measure was only introduced in financial year 2025 and there have been no reports from employees in the value chain since then, we do not yet have any data on its effectiveness.

S2-4 Actions

As part of the materiality assessment, secunet did not identify any significant potential or actual, positive or negative impacts on employees in the value chain.

The risk analysis conducted in accordance with the German Supply Chain Due Diligence Act (LkSG) shows that, due to the geographical structure of the supply chain – with direct suppliers in Europe – there are currently no prioritized human rights or labor law (LkSG) risks. Should relevant indications of (LkSG) risks become apparent in the future, secunet will analyze them and take appropriate measures.

Supply Chain Compliance Management System (L-CMS)

secunet is a signatory to the UN Global Compact and commits itself, through its policy statement, to respecting and promoting human rights. This statement is a central component of the company-wide supply chain compliance management system (L-CMS), which ensures that human rights and environmental due diligence obligations are met throughout the entire value chain. The implementation of the L-CMS is a dynamic, ongoing process.

A key component of the L-CMS is the annual and ad-hoc LkSG risk analysis. The aim is to identify potential risks early on, especially for vulnerable workers.

Continuous abstract risk analyses, taking into account country- and industry-specific factors, form the basis for the concrete assessment and monitoring of risks in the supply chain. ESG risk management software supports the automated review of direct suppliers for compliance with human rights and environmental standards. The final risk assessment is based on the probability and severity of potential violations, the impact on identified risks, and the respective supplier's contribution to the risk.

Complaints procedures and remedies

To promote transparency regarding risks in the supply chain, the company-wide whistleblower system has been supplemented with a complaint procedure in accordance with Section 8 of the German Supply Chain Due Diligence Act (LkSG). This allows employees in the value chain to report human rights and environmental violations, either by providing their name or anonymously.[10]

Should the LkSG risk analysis identify risks at a supplier, remedial actions will initially be developed in cooperation with the affected suppliers. If necessary, these can be supplemented by further measures such as audits.[11]

The actions described were first implemented in financial year 2024. An assessment of their effectiveness will therefore only be possible in the coming years and will be based on a risk-based analysis.

[10] Further details on the complaints procedure and its effectiveness assessment are described in section S2-3.
[11] Further details regarding the corrective measures are described in section S2-3.

S2-5 Targets

In our ESG strategy, we have formulated a target developed by the Compliance department in collaboration with the Sustainability department and the Supply Chain Management and Procurement departments. This target is intended to contribute to the management of material risks. The target was agreed upon by the Director of Sustainability and the Management Board.

Sustainability assessment of all high-risk suppliers

Description: By 2028, 100% of high-risk direct suppliers should have completed an ESG assessment.

Sustainability is assessed via an ESG assessment. Only suppliers deemed to pose a risk are invited to participate in the ESG assessment.

Suppliers with medium or high abstract country and/or industry risk are considered high-risk. This classification takes into account the supplier class and – for suppliers who are not strategically important – an annually determined threshold for purchasing volume. Class C suppliers are only considered if they exhibit a high level of risk. Only suppliers with an active business relationship are considered.

A supplier is considered assessed once the questionnaire has been fully completed, regardless of the specific answers chosen. Alternatively submitted equivalent evidence, such as an EcoVadis rating or relevant certifications, will also be accepted.

The response rate is calculated as the ratio of suppliers considered to be rated to the total number of suppliers deemed to be at risk.

Assumptions: A completed ESG assessment of our high-risk suppliers enables the prioritization of identified risks and the early definition of targeted prevention and remediation measures to counteract the risk of non-compliance with social standards.

Time horizon: ongoing

Monitoring of the target: Progress regarding the defined KPI is collected annually by the Corporate Compliance department and shared with the members of the Management Board in the annual report.

Base year 2025: 93.75%

Involvement of workers in the value chain: The perspective of the workforce in the value chain or their legal representatives or credible proxies was not taken into account when setting the target.

Governance

ESRS G1 – Business conduct[12]

Disclosure requirements in connection with ESRS 2 SBM-3 – Material impacts, risks and opportunities and their interaction with strategy and business model

IROs

Sub-sub-matters			Position in the value chain			Time horizon		
			Upstream	Own activities	Downstream	Short term	Medium term	Long term
Corporate culture	**Promoting corporate culture** A positive corporate culture raises employee awareness of ethical behavior and strengthens trust between employees and business partners. This creates a sustainable and integrity-oriented work environment that promotes social responsibility both within and outside the company.	Actual positive impact		X				X
Protection of whistleblowers	**Protection of whistleblowers** secunet's group-wide whistleblower system, fostered by an integrity-oriented corporate culture, strengthens the willingness of employees and third parties to confidentially report unethical behavior. This ensures reliable protection for whistleblowers, early risk identification, and support for compliance with legal and internal regulations.	Actual positive impact	X	X	X			X
Corruption and bribery	**Risk from corruption** As an IT security service provider with a focus on the public sector, secunet is particularly dependent on trust, integrity, and regulatory compliance. Corruption incidents could lead to exclusion from tendering processes, severe sanctions, and serious reputational damage with direct financial consequences.	Risk		X				X
Political influence and lobbying activities	**Non-compliance with regulations** Anti-competitive practices such as aggressive lobbying, illegal agreements, or the exploitation of dominant market positions can increase procurement costs, stifle innovation, and reduce the quality of safety-critical products. This would not only lead to financial losses but also reputational damage and could significantly undermine customer trust, particularly in the public sector.	Risk		X			X	

The list of IROs highlights sustainability issues that, if inadequately managed, could pose risks for secunet. However, the impacts can also be positive.

[12] Since the company's overarching ESG strategy is still under development, no quantitative targets have yet been defined for individual governance aspects. As the ESG strategy matures, quantitative targets will be developed and implemented gradually.

G1-1 – Corporate culture

Material impacts and their interaction with the strategy and business model

As part of the materiality assessment, a genuine positive impact was identified for the matter of "Corporate culture" within the company's own business area. An integrity-oriented corporate culture raises employee awareness of ethical behavior, strengthens trust between employees and business partners, and creates a sustainable work environment that promotes social responsibility both within and outside of secunet. This is based on the company values developed and published in 2022, which have since provided guidance for daily operations.

This impact is closely linked to secunet's strategy and business model. As an IT security service provider primarily serving the public sector, secunet relies heavily on trust, integrity, and regulatory compliance. An integrity-oriented corporate culture supports secunet in meeting these requirements and upholding its core promise as a reliable and law-abiding partner. The ESG strategy adopted in 2025 underscores this by highlighting corporate culture, integrity, and compliance as essential components within the Governance (G) dimension. Measures such as the group-wide Code of Conduct for employees, the Compliance Management System (CMS), and diverse internal communication and exchange formats foster this corporate culture and ensure its positive long-term impact.

Policies: Corporate culture

Code of conduct for employees

A key element of the compliance management system is the group-wide Code of Conduct for Employees, which is binding for all employees. This code was updated in 2025, adopted by the secunet Management Board, and put into effect. The Code of Conduct aims to promote and ensure sustainable and responsible conduct in daily work. Its content is based on internationally recognized standards, such as the ILO norms. Above all, it seeks to foster a positive and ethical corporate culture that raises employee awareness of ethical behavior. Compliance with the Code is of paramount importance; violations will not be tolerated and will be sanctioned accordingly. The Code of Conduct is available in German and English on the intranet and website for employees and third parties.

The code of conduct for employees includes binding rules of conduct regarding human rights, social standards, labor standards, environmental protection, transparent and sustainable business relationships, fair market behavior, information security and data protection.

Various corporate and company guidelines, as well as work instructions, supplement and specify legal and internal requirements from the code of conduct for employees. These are also binding for all employees.

Actions: Corporate culture

secunet values

secunet's corporate culture is a key element of our shared success and is based on five core values developed and defined by the company's employees in a values workshop in 2022. These values were published by the Management Board at the end of 2022 and have since served as a guide for daily operations and the company's long-term direction.[13]

[13] Unless otherwise stated, all measures mentioned in this section are ongoing.

Social days

To actively embody and further develop its corporate values, secunet is involved in non-profit, hands-on projects throughout Germany, such as redesigning the spaces and outdoor areas of project partners, and organizing excursions with children and young people from these partner organizations. Since 2023, the company has held annual Social Days at its large and small locations, giving all employees the opportunity to engage in social activities. These activities aim to strengthen team spirit and cohesion, and contribute to making the company values tangible.

secunet summit

Furthermore, the secunet summit offers employees a valuable opportunity to connect and network across divisions, departments, and locations. The focus is not only on professional exchange but also on fostering cohesion within the company. In addition to collaboratively developing company-relevant topics, great emphasis is placed on inspiring discussions and a diverse program of activities that highlights the fun and enjoyment of working together. Since 2022, the secunet summit has been held every three years to ensure this unique experience continues regularly.

Communication and exchange formats

Open and regular internal communication forms the backbone of our corporate culture. Formats such as all-hands meetings, blog posts from the board and specialist departments, and company-wide news promote transparency and make our corporate values tangible. Blog posts offer exciting insights into current projects, successes, and innovations, strengthen knowledge transfer, and create a vibrant connection between the various areas of secunet.[14]

secunet places great importance on the personal and professional development of its employees. Training courses, workshops, and exchange formats specifically promote skills, strengthen identification with secunet, and contribute to employee motivation and satisfaction.[15]

Corporate culture is assessed through employee surveys. These surveys provide insights into employee satisfaction and engagement, helping to analyze perceptions of the corporate culture and identify potential areas for improvement. In 2025, additional questions were included in the employee survey to capture the compliance and integrity culture within the secunet Group. The results are expected by mid-2026 and will subsequently be communicated internally to employees.[16]

Compliance management system

A key component of this is our compliance management system, which the secunet Management Board implemented for damage prevention and risk control. With this system, secunet establishes uniform standards across the group for essential compliance issues, thereby ensuring that secunet acts in accordance with applicable legal regulations in the countries where it operates.

The principles and measures implemented with the CMS encompass the essential elements of a compliance management system according to IDW PS 980. All measures reflect the "tone from the top" set by the Management Board.[17]

In 2022, the adequacy and effectiveness of the compliance management system were certified by an external audit in accordance with IDW Auditing Standard 980. For the 2025 financial year, the adequacy and effectiveness of the compliance management system were reviewed, as in the previous financial year, through a self-assessment.

The overall responsibility for the implementation, monitoring, and further development of the CMS lies with the secunet Management Board. The operational implementation and monitoring of compliance measures has been delegated to the Compliance Office, which also serves as the central point of contact and steering unit for compliance issues within the secunet Group.

[14] For further information see ESRS S1-2.
[15] For further information see ESRS S1-4.
[16] For further information on the employee survey and its results for 2024, see ESRS S1-1 & S1-2.
[17] The Tone from the Top can be found under the heading "Corporate Compliance" on the secunet website: https://www.secunet.com/ueber-uns/unternehmen

Compliance training

All employees are required to participate in digital training sessions on compliance topics every two years. These sessions aim to raise employee awareness of ethical and legally sound conduct. The compliance training sessions last between 15 and 45 minutes.

Training courses are offered on the following topics:

- Fundamentals of compliance
- Antitrust law
- Dealing with conflicts of interest
- Corruption prevention
- Data protection
- Prevention of insider trading

Currently, no measurable, results-oriented targets in line with the ESRS have been defined for the matter of "Corporate culture." The effectiveness of management policies and actions in terms of their positive impact is not currently being tracked.

Protection of whistleblowers

Material impacts and their interaction with the strategy and business model

In the materiality assessment, the protection of whistleblowers was assessed as material due to its demonstrably positive impact. This identified impact relates to the company's own business operations as well as to the upstream and downstream value chain. Through an integrity-oriented corporate culture, secunet strengthens the willingness of employees and third parties to report unethical behavior or potential violations. Our group-wide whistleblower system enables both internal and external whistleblowers to confidentially report incidents and reliably protects them from repercussions. In this way, secunet contributes to risk prevention, protects those harmed, and supports compliance with legal and internal company regulations.

Whistleblower protection is an essential component of the compliance management system and is firmly anchored in the governance dimension of the ESG strategy. The whistleblower system is based on the requirements of EU Directive 2019/1937 and the Whistleblower Protection Act, and also takes into account the German Supply Chain Due Diligence Act (LkSG). In addition, a procedural guideline and internal processes have been implemented to ensure a uniform, legally compliant handling of reports and to promote a positive long-term impact.

Policies: Protection of whistleblowers

Whistleblower system

The whistleblower system is addressed both in the group guidelines of the Corporate Compliance department and in the code of conduct for employees and code of conduct for suppliers and business partners.

All employees of the secunet Group can find information about the whistleblower system and the complaints procedure on the intranet. The individual reporting channels and categories are explained there. Information about the whistleblower system is also provided in blog posts. New employees are also made aware of the whistleblower system via an onboarding email.

Furthermore, the secunet Group has a code of procedure designed to ensure a fair and transparent process that respects both the principle of proportionality for those affected and the protection of the whistleblower. This code of procedure applies to all individuals who submit reports under the Disclosure Protection Act (HinSchG) and complaints under the German Supply Chain Due Diligence Act (LkSG) and is available on the secunet website and intranet. It was enacted by the Management Board. The Compliance Officer is responsible for the operational implementation of this code of procedure. Five internal reporting channels exist for whistleblowers to report violations. Reports and violations can be submitted via email, the electronic whistleblower system, mail, in person, and/or by telephone. The content of this code of procedure is based on the provisions of the Disclosure Protection Act (HinSchG) and the German Supply Chain Due Diligence Act (LkSG).[18]

The reporting officers continuously deepen their expertise through specialized training courses and webinars on internal investigations and whistleblower systems. Furthermore, they constantly monitor relevant legal and regulatory developments and engage in professional exchange on best practices within relevant networks.

Actions: Protection of whistleblowers

The secunet Group prohibits and will not tolerate any form of retaliation (e.g., adverse measures, disciplinary action, threats, intimidation) against individuals who report in good faith. To protect our whistleblowers, employees are offered the option of contacting external reporting bodies (e.g., BaFin, BAFA) or reporting anonymously via various internal reporting channels.

Furthermore, all reports of rule violations and complaints, as well as all information contained therein, are treated with strict confidentiality. The whistleblower's identity is protected with the utmost care. The investigation of whistleblower reports or complaints follows the "need-to-know" principle, meaning that only those individuals necessary for clarifying the facts are involved. Care is taken to ensure that the report/complaint, the individuals involved, and the facts presented are used in anonymized and generalized form for further processing, research, and clarification.

[18] For further information on the contents of the procedural instruction, see ESRS S2-3.

Reports of violations (incidents/breaches) of legal and company regulations, including those related to corruption and bribery, can be submitted to the Corporate Compliance department via the whistleblower system. The reporting office investigates these cases immediately (in compliance with legal requirements), independently, separately from the management chain, and according to the principle of "no one should judge their own case". All internal investigations are conducted fairly, transparently, and objectively, respecting the rights of all parties involved and without any bias. The principle of presumption of innocence always applies to ensure a fair and legally compliant examination of the facts.

Targets: Protection of whistleblowers

For the matter of "Protection of whistleblowers," no measurable, results-oriented targets as defined by the ESRS are currently in place. The effectiveness of management policies and actions with regard to their positive impact is not currently being tracked. See the explanation in section S2-3.

G1-3 – Prevention and detection of corruption and bribery

Material impacts and risks and their interaction with the strategy and business model

Risks

Corruption incidents would not only lead to high fines, sanctions, and increased compliance costs, but above all, they would undermine the company's core promise to be a reliable and law-abiding partner. Reputational damage in this environment could have serious consequences, including declines in sales revenue and EBIT, the loss of strategic customer relationships, and difficulties in initiating future business in the core market.

For secunet, preventing and detecting corruption is of paramount importance, as its business model relies heavily on public tenders. Trust, integrity, and regulatory compliance are essential prerequisites for operating successfully in its core market and securing long-term customer relationships. Even the mere suspicion of corruption can lead to exclusion from tendering processes, thus directly jeopardizing business success. Therefore, the anti-corruption program is not only part of the compliance organization but also strategically embedded in corporate governance. Furthermore, it forms a central component of the ESG strategy (governance dimension) and supports the goal of positioning secunet as a reliable, law-abiding, and responsible partner in the public sector and beyond.

Policies: Prevention and detection of corruption and bribery

As an active participant in the UN Global Compact Germany, secunet is committed to combating and preventing corruption and bribery in all its forms. Our zero-tolerance policy is enshrined in our Code of Conduct for employees as well as in our Code of Conduct for suppliers and business partners.[19]

Anti-corruption policy

This principle is also enshrined in the separate, group-wide internal anti-corruption policy, which was updated in financial year 2025 and adopted by the Management Board. It serves to proactively prevent corruption risks and provides employees with clear guidelines for their daily work. The anti-corruption policy is based on the requirements of internationally recognized standards such as the UK Bribery Act and the Foreign Corrupt Practices Act (FCPA). It contains binding guidelines for handling gifts in the private sector and to public officials, which, in response to various employee inquiries, have been further clarified in the new version by means of a graphical decision table. The policy also governs the application for donations and sponsorships, as well as the engagement of external personnel. Supplementary process descriptions ensure consistent implementation.

The anti-corruption policy applies to all employees in all group companies and is available on the intranet. It is reviewed annually and is an integral part of the internal control system (ICS) and the compliance management system. Compliance with the policy is monitored by internal audit as part of its ongoing audits.

Actions: Prevention and detection of corruption and bribery

Communication measures:

The Compliance Office uses various communication channels (intranet, emails or a group-wide compliance blog) to inform employees about relevant requirements regarding anti-corruption or other regulatory changes.

Advice

The Corporate Compliance department advises employees on issues relating to integrity and compliance, as well as on anti-corruption, supply chain and human rights, and antitrust law.

Monitoring and audits

To detect violations, compliance audits were conducted in cooperation with Internal Audit. For the first time in financial year 2024, compliance with legal and company-internal requirements was reviewed through compliance audits in the subsidiaries, and measures were derived and recommendations issued based on the findings.

Reporting channels and whistleblower system

The anti-corruption policy defines clear reporting channels and contact persons for reporting potential violations or obtaining further advice. Suspected cases can be reported anonymously or with personal information via the whistleblower system. This enables the systematic identification, investigation, and prosecution of violations, allowing corruption risks to be detected early and effectively addressed.

Compliance violations are reported annually and on an ad hoc basis to the Management Board and the Supervisory Board/Audit Committee.

[19] For further information see ESRS S1-1.

Training courses on corruption prevention

Employees are taught compliant and ethical conduct through mandatory training courses held every two years. These courses, which focus on corruption prevention, cover topics such as anti-corruption measures and managing conflicts of interest. Information and guidance on these topics are also available on the intranet.

The training courses on anti-corruption and dealing with conflicts of interest cover the following topics:

- Handling of gifts from public officials
- Handling donations from the private sector
- Identifying and preventing conflicts of interest in the professional environment
- Risks and effects of conflicts of interest
- Dealing with conflicts of interest

Training in anti-corruption and conflict management is mandatory for all employees. This means that 100% of high-risk functions are covered by the two training modules. Due to their interfaces with external business partners, the marketing, sales, and purchasing departments are considered high-risk areas with regard to corruption and bribery. Management bodies also receive training through these two modules. secunet does not currently offer separate training for the Supervisory Board.

Targets: Prevention and detection of corruption and bribery

In our ESG strategy, we have formulated overarching targets, which were developed by the Compliance department in collaboration with the Sustainability department. These targets are intended to contribute to managing material risks and promoting positive impact. The targets were agreed upon by the Director of Sustainability and the Management Board.

Training rate

Description:

By 2030, 100% of all employees in the secunet Group are expected to have successfully completed mandatory training on corruption prevention and managing conflicts of interest. The annual KPI indicates the percentage of employees who have completed the respective training courses within the prescribed two-year cycle.

The Corporate Compliance department determines the training rate annually based on the employee numbers submitted by the Human Resources department.

The training rate is calculated separately for each training module and results from the ratio of employees who have successfully completed the respective training module within the last two years to the total number of employees of the secunet Group as of December 31st.

Assumptions:

A consistently high training rate documents the implementation of preventive CMS measures and contributes to a broad risk awareness among employees. It demonstrates the effective integration of the CMS within the company and strengthens the integrity-oriented corporate culture through the systematic prevention of legal and policy violations, thereby also counteracting the risk of corruption incidents.

Time horizon:

ongoing

Monitoring the target:

The training rates are documented in the annual report and presented to the Management Board and Supervisory Board/Audit Committee.

Target achievement by 2025:

Target: 95% per module
Actual: 95.48% (corruption prevention)
96.70% (Handling of conflicts of interest)

Intermediate goal:

2028: 97.5% per module

Base year 2024:

Corruption prevention: 95.22%
Handling of conflicts of interest: 93.44%

Integration of employees into the value chain:

Since this is an exclusively internal measure, there are no interactions with employees in the upstream and downstream value chain.

Key figures: Detection and prevention of corruption and bribery

Training rates for the "Anti-Corruption" and "Dealing with conflicts of interest" courses[20]

	Organs (VS+GF)	Managers	Risk-exposed roles	Other employees
Coverage through "Corruption prevention" training				
Total	11	173	130	990
Trained persons	11	168	127	939
Training rate	100.00%	97.11%	97.69%	94.85%
Coverage through training on "Dealing with conflicts of interest"				
Total	11	173	130	990
Trained persons	11	168	127	955
Training rate	100.00%	97.11%	97.69%	96.46%
Training method and duration				
Computer-based training	30 min	30 min	30 min	30 min
Frequency	every 2 years	every 2 years	every 2 years	every 2 years

Number of convictions and the amounts of fines

Number of convictions for violations of corruption and bribery regulations	0
Amount of fines for violations of corruption and bribery regulations	0

[20] Including the Management Board. To avoid double counting, employees are assigned to categories that are unique and mutually exclusive. Multiple assignment to several categories is not permitted.

G1-5 – Political influence and lobbying activities

Material impacts and risks and their interaction with the strategy and business model

In the materiality assessment, the matter of "Political influence and lobbying activities" was assessed as material due to a specific risk. This risk relates exclusively to the company's own business operations. Anti-competitive practices such as aggressive lobbying, unlawful agreements, or the abuse of dominant market positions can increase procurement costs, stifle innovation, and compromise the quality of safety-critical products. In addition to financial disadvantages, such behavior would also lead to significant reputational damage and jeopardize customer trust, particularly in the public sector. Furthermore, there is a risk that legal restrictions on lobbying activities or a diminishing influence on political decision-making processes could limit secunet's ability to respond to regulatory developments in a timely manner.

As a company whose business model relies heavily on public tenders, secunet depends on integrity, transparency, and trust. Political advocacy is not about pushing through one-sided corporate interests, but rather about constructively shaping framework conditions that strengthen the resilience and security of the digital society.

As the IT security partner of the Federal Republic of Germany, secunet is committed to the continuous development of its technologies to ensure a high level of confidentiality and integrity for the communication infrastructures of companies and public authorities. Against this backdrop, secunet maintains an open dialogue with policymakers and public administrations – particularly regarding IT and cybersecurity issues, as well as digital infrastructures. Regular exchanges with federal ministries and members of the German Bundestag clarify technical topics and identify necessary changes that are of central importance to the framework for business operations and, consequently, for employees. This transparent approach reinforces secunet's position as a reliable partner of the public sector and contributes to its long-term competitiveness.

Policies: Political influence and lobbying activities

Antitrust Directive

A key foundation for the secunet Group's lobbying activities is the Antitrust Policy, which defines specific requirements for dealing with political decision-makers and institutions. It ensures that all lobbying activities are conducted in compliance with regulations, transparently, and in accordance with applicable antitrust provisions. This includes clear internal processes for managing and monitoring lobbying efforts to avoid risks such as undue influence or anti-competitive cooperation.

The directive aims to prevent antitrust violations and suspected violations, and to maintain confidence in the lawful conduct of secunet and its employees. The directive is designed to implement applicable German (e.g., amendments to the German Competition Act) and European antitrust law.

It establishes binding standards for compliance with national and European competition rules and provides clear guidelines for dealing with competitors, customers, and suppliers. It also regulates conduct in cases of dominant market position and during regulatory investigations (dawn raids).

All employees are required to participate regularly in antitrust training. Participation is monitored and documented by the Corporate Compliance department. In addition, the whistleblower system offers the opportunity to report potential violations anonymously or with personal information. This system helps to identify, investigate, and effectively address risks at an early stage.[21]

The policy, last updated in 2025 and approved by the Management Board, applies to all secunet Group companies and employees. The Corporate Compliance department, with support from the Legal department, is responsible for the operational implementation of the policy. The antitrust policy is available to employees on the intranet. It serves as a fundamental minimum standard for all company activities, is an integral part of the compliance management system, and is reviewed annually. Compliance with the policy is verified by internal audit.

[21] For further information on compliance training, see G1-1.

Actions: Political influence and lobbying activities

Lobby register

secunet is registered in both the German lobby register and the EU transparency register, thus committing itself to transparent and responsible lobbying.

Transparency Register	Registration number
EU Transparency Register	533422038902-36
Lobby register for lobbying vis-à-vis the German Bundestag and the Federal Government	R001612

Public affairs

The CEO has ultimate responsibility for overseeing lobbying activities within the secunet Group, but has delegated operational implementation to the Public Affairs department. The Public Affairs department is responsible for developing strategies to represent the secunet Group's interests in the political arena. Furthermore, the Public Affairs department advises and supports management in its communication and advocacy efforts with political decision-makers.

secunet participates in numerous industry associations and advocates for a fair competitive environment. In doing so, secunet ensures that all political lobbying activities comply with antitrust regulations. The goal is to promote framework conditions that strengthen innovation and safety without harming competition.

Objectives: Political influence and lobbying activities

For the matter of "Political influence and lobbying activities," no measurable, results-oriented targets as defined by the ESRS have been established. The effectiveness of management policies and actions in relation to this risk is not currently being monitored.

Key figures: Political influence and lobbying activities

Financial expenditures for lobbying activities

In the completed financial year 2025, the secunet Group's financial expenditures for lobbying activities in Germany totaled €155,200. This amount includes rounded figures for pro rata personnel costs, infrastructure costs, representation costs, external consulting and support services, and other costs, including association membership fees.[22,23,24]

A total of €119,000 was spent on lobbying activities with European Union organizations – excluding EU member states. This sum comprises a share of personnel costs, travel expenses, external consulting and support services, membership fees, and back-office and administrative costs.

[22] The information on financial benefits is based on internal company surveys.
[23] Analogous to the requirements of the Lobby Register Act, a factor of 0.3 was used to determine personnel costs.
[24] The amount of lobbying expenditure that the individual associations plan to allocate for the 2025 financial year has not yet been determined. The calculations were based on figures from the 2024 financial year.

Company-specific matters

Information security

secunet's customers are primarily in the public sector, including national and international governments, ministries, agencies, and quasi-governmental organizations. The company also focuses on the German Armed Forces, security authorities such as the police and border patrol, and sectors with high IT security requirements, such as healthcare, critical infrastructure, and industrial companies.

Our customers strive for digital sovereignty – that is, secure and trustworthy control over their data. With solutions for administrative digitalization and the digitalization of the German Armed Forces, secunet makes a significant contribution to national sovereignty by enabling the secure processing of (state) secrets.

Through its product portfolio, secunet supports societal concerns such as data protection, information security, and digital sovereignty. Data protection and informational self-determination are fundamental rights in the EU; information security is an essential prerequisite for this. Digital sovereignty means shaping digitalization without creating new structural, economic, or political dependencies – and here, too, information security plays a central role.

As part of the materiality assessment, we have identified a key company-specific issue in connection with our clients: this is the issue of information security, which materializes in the form of cybersecurity, data protection and data security.

The following impacts, risks, and opportunities have been identified:

IROs		Position in the value chain			Time horizon		
		Upstream	Own Activities	Downstream	Short term	Medium term	Long term
Contribution to information and data security secunet is a trusted provider in the field of IT security and ensures trustworthy digitalization.	Actual positive impact	X	X	X	X	X	X
Sustained demand for secunet products Effective, reliable IT security ensures trustworthy digitalization for customers, sustained demand for secunet products, and thus long-term business success for secunet.	Opportunity		X		X	X	X
Loss of trust Systematic weaknesses destroy trust in secunet and its business model, which can lead to a decline in orders and revenue losses.	Risk		X		X	X	X

The list of IROs includes sustainability aspects which, if not handled appropriately, can lead to advantages and disadvantages for customers (positive and negative impacts) and to potential positive and negative financial impacts (opportunities and risks).

There are therefore many interactions between IROs and strategy and business model.

Information and data security is a core element of secunet's strategy and business model. This means that our strategy and business model are closely linked to their actual impact on our customers.

The main risks and opportunities associated with information security arise from the trust our customers place in us: security gaps can lead to a loss of trust, customer churn, and declining revenue; conversely, high reliability and customer satisfaction create sustainable business relationships. Rapid problem resolution and high product quality mitigate risks and enhance opportunities.

Policies

Information security is at the heart of our products and services. It forms the basis for data protection and the digital sovereignty of our customers. In addition to technical implementation, particularly cryptographic methods, secunet offers organizational consulting in accordance with the GDPR.

Our IT security partnership with the Federal Republic of Germany, as well as numerous products approved and certified by the Federal Office for Information Security (BSI), demonstrate this commitment. secunet also supports its customers' data security through consulting services in information security management and data protection.

The increasing digitalization in the cloud links IT security with digital sovereignty. With the SINA Cloud, secunet has developed a certifiable cloud platform that enables customers to operate highly secure and independent cloud infrastructures. The security mechanisms of the SINA Cloud were approved in 2024 for processing classified information up to the SECRET classification.

secunet also adheres to the highest internal standards in data protection and data security. Processes, systems, and responsibilities are certified according to ISO/IEC 27001:2024. The continuous development of technical and organizational security measures ensures data protection at the highest level. Data security requirements are also passed on to suppliers via the terms and conditions.

The concept's scope encompasses the entire value chain, from development and procurement to customer use. In the upstream chain, technical specifications are reviewed; in the downstream chain, customer feedback is systematically evaluated.

The Management Board of secunet AG decides on the product and service strategy. Product management, development, quality assurance, purchasing, supply chain management, and quality management are responsible for its implementation. Implementation is monitored by the respective departments of the Management Board.

Customers and stakeholders are involved in various ways, e.g. through close cooperation with the BSI, regular coordination on needs and requirements, and through feedback from commissioned developments.

Actions

The most important actions for ensuring positive impacts consist of providing secure products and solutions, as well as supplementary advice on technical and organizational data protection actions. Quality assurance, approval processes, and incident management guarantee the effectiveness of these actions.

Action plans and resource allocations are part of the internal product strategy and are confidential. The resources used for this purpose consist primarily of personnel costs in product management, development, quality assurance, regulatory affairs, sales, and customer support.

Indications of potential security vulnerabilities are collected via customer support, the BSI (Federal Office for Information Security), or industry channels, evaluated, and addressed with appropriate actions – such as communication,

updates, or bug fixes. These actions undergo internal quality assurance and, if necessary, BSI approval.

These actions are ongoing and apply to all customers and end users. The associated expenses and investments correspond to the amounts reported in the annual financial statements. No specific targets were set for the individual actions. The effectiveness of the actions is reflected in customer satisfaction, market acceptance, and business success.

Customer satisfaction: NPS and CRI

We conduct a customer satisfaction survey annually.

For this purpose, the Net Promoter Score (NPS) is calculated. The NPS is a method for easily measuring customer satisfaction with a specific brand or company and its products: A short survey asks customers about their willingness to recommend the brand or company. The goal is to maintain or exceed the previous year's NPS.

On a scale of 0 to 10, respondents can indicate their agreement with the simple question, "Would you recommend secunet to others?" All respondents who choose 0 to 6 are considered to be "critics", ratings of 7 and 8 are disregarded, and only those who choose 9 or 10 are counted as "promoters." An index is then calculated: % Promoters - % Critics = NPS, with a value between -100 and +100. This serves as an indicator of customer loyalty and retention.

However, the NPS is statistically unreliable and remains vague. Therefore, we also determine the Customer Retention Index (CRI) using four additional questions (overall satisfaction, continuation of the customer relationship, perceived competitive advantage, likelihood of recommendation). This provides us with further information on the degree of customer loyalty (based on an index number).

Both indicators increased in 2025 compared to 2024.

Customer satisfaction indicator	2022	2023	2024	2025
NPS	17	33	17	28
CRI	70	78	71	76

Data points from EU legislation

The following table contains the data points derived from other EU legislation, as listed in Annex B of ESRS 2. It shows where these data points can be found in our report and identifies those that have been classified as "not material".

- **Not material:** information not material to reporting.
- **Not relevant:** information not relevant to business operations.

Disclosure requirement	Data point	Description	SFDR reference	Pillar 3 reference	Benchmark regulation reference	EU climate law reference	Page / Materiality
ESRS 2 GOV-1	21 (d)	Board's gender diversity	x		x		p. 37
ESRS 2 GOV-1	21 (e)	Percentage of board members who are independent			x		p. 38
ESRS 2 GOV-4	30	Statement on due diligence	x				p. 39
ESRS 2 SBM-1	40 (d) i	Involvement in activities related to fossil fuel	x	x	x		Not relevant
ESRS 2 SBM-1	40 (d) ii	Involvement in activities related to chemical production	x		x		Not relevant
ESRS 2 SBM-1	40 (d) iii	Involvement in activities related to controversial weapons	x		x		Not relevant
ESRS 2 SBM-1	40 (d) iv	Involvement in activities related to the cultivation and production of tobacco			x		Not relevant
ESRS E1-1	14	Transitional plan to reach climate neutrality by 2050				x	Not relevant
ESRS E1-1	16 (g)	Undertakings excluded from the Paris-aligned benchmarks		x	x		Not relevant
ESRS E1-4	34	GHG emission reduction targets	x	x	x		Not relevant
ESRS E1-5	38	Energy consumption from fossil fuels broken down by source (high climate impact sectors only)	x				Not relevant
ESRS E1-5	37	Energy consumption and energy mix	x				p. 56
ESRS E1-5	40-43	Energy intensity associated with activities in high climate impact sectors	x	x			Not relevant
ESRS E1-6	44	Gross GHG emissions of Scope 1, 2 and 3, as well as total GHG emissions	x	x	x		p. 57
ESRS E1-6	53-55	Intensity of gross greenhouse gas emissions	x		x		p. 61
ESRS E1-7	56	Removal of greenhouse gases and carbon certificates				x	Not relevant
ESRS E1-9	66	Exposure of the benchmark portfolio to climate-related physical risks			x		Not relevant

Disclosure requirement	Data point	Description	SFDR reference	Pillar 3 reference	Benchmark regulation reference	EU climate law reference	Page / Materiality
ESRS E1-9	66 (a); 66 (c)	Disaggregation of monetary amounts by acute and chronic physical risk. Location of significant assets at material physical risk	x				Not relevant
ESRS E1-9	67 (c)	Breakdowns of the carrying value of its real estate assets by energy-efficiency classes		x			Not relevant
ESRS E1-9	69	Degree of portfolio exposure to climate-related opportunities			x		Not relevant
ESRS E2-4	28	Amount of each pollutant listed in Annex II of the E-PRTR Regulation (European Pollutant Release and Transfer Register) emitted to air, water and soil	x				Not material
ESRS E3-1	9	Water and marine resources	x				Not material
ESRS E3-1	13	Dedicated policy	x				Not material
ESRS E3-1	14	Sustainable oceans and seas	x				Not material
ESRS E3-4	28 (c)	Total amount of recovered and reused water	x				Not material
ESRS E3-4	29	Total water consumption in m3 per net revenue from own activities	x				Not material
ESRS 2 - SBM 3 - E4	16 (a) i	—	x				Not material
ESRS 2 - SBM 3 - E4	16 (b)	—	x				Not material
ESRS 2 - SBM 3 - E4	16 (c)	—	x				Not material
ESRS E4-2	24 (b)	Sustainable practices or policies in the field of land use and agriculture	x				Not material
ESRS E4-2	24 (c)	Sustainable processes or policies in the field of oceans/seas	x				Not material
ESRS E4-2	24 (d)	Policies to address deforestation	x				Not material
ESRS E5-5	37 (d)	Non-recycled waste	x				p. 64
ESRS E5-5	39	Hazardous and radioactive waste	x				Not relevant
ESRS 2 - SBM3 - S1	14 (f)	Risk of forced labor	x				Not relevant
ESRS 2 - SBM3 - S1	14 (g)	Child labor	x				Not relevant
ESRS S1-1	20	Commitments in the area of human rights policy	x				p. 75
ESRS S1-1	21	Due diligence policies on issues addressed by the fundamental conventions 1 to 8 of the International Labour Organization			x		p. 75
ESRS S1-1	22	Processes and measures to prevent human trafficking	x				p. 75
ESRS S1-1	23	Workplace accident prevention policy or management system	x				p. 75
ESRS S1-3	32 (c)	Grievance/complains handling system	x				p. 76
ESRS S1-14	88 (b) & (c)	Number of fatalities and number and rate of work-related accidents	x		x		p. 81

Disclosure requirement	Data point	Description	SFDR reference	Pillar 3 reference	Benchmark regulation reference	EU climate law reference	Page / Materiality
ESRS S1-14	88 (e)	Number of days lost due to injuries, accidents, fatalities or illness	x				p. 81
ESRS S1-16	97 (a)	Unadjusted gender pay gap	x		x		p. 82
ESRS S1-16	97 (b)	Excessive remuneration of members of the management bodies	x				p. 82
ESRS S1-17	103 (a)	Incidents of discrimination	x				p. 82
ESRS S1-17	104 (a)	Non-compliance with the United Nations Guiding Principles on Business and Human Rights and the OECD Guidelines	x		x		p. 82
ESRS 2 - SBM3 - S2	11 (b)	Significant risk of child labor or forced labor in the value chain	x				p. 83
ESRS S2-1	17	Commitments in the area of human rights policy	x				p. 84
ESRS S2-1	18	Policies related to workers in the value chain	x				p. 84
ESRS S2-1	19	Non-compliance with the United Nations Guiding Principles on Business and Human Rights and the OECD Guidelines			x		p. 84
ESRS S2-1	19	Due diligence policies in relation to issues addressed in Fundamental Conventions 1 to 8 of the International Labour Organization	x				p. 84
ESRS S2-4	36	Human rights issues and incidents within the upstream and downstream value chain	x				p. 86
ESRS S3-1	16	Human rights policy commitments	x				Not material
ESRS S3-1	17	Non-compliance with the United Nations Guiding Principles on Business and Human Rights, the ILO Principles, or the OECD Guidelines	x		x		Not material
ESRS S3-4	36	Human rights issues and incidents	x				Not material
ESRS S4-1	16	Policies related to consumers and end users	x				Not material
ESRS S4-1	17	Non-compliance with the United Nations Guiding Principles on Business and Human Rights and the OECD Guidelines	x		x		Not material
ESRS S4-4	35	Human rights issues and incidents	x				Not material
ESRS G1-1	§10 (b)	United Nations Convention against Corruption	x				p. 90
ESRS G1-1	§10 (d)	Protection of whistleblowers	x				p. 92
ESRS G1-4	§10 (d)	Fines for offences against corruption and bribery regulations	x		x		p. 96
ESRS G1-4	§24 (b)	Standards of anti-corruption and anti-bribery	x				p. 94

Report of the Management Board pursuant to Section 312 (3) AktG

Pursuant to Section 312 (3) of the German Stock Corporation Act (AktG), the Management Board has issued a report on the relations with affiliated companies for the 2025 financial year. The report contains the following closing statement: "It is hereby declared that, according to the circumstances known to the Management Board at the time the respective legal transactions were undertaken, our Company received an appropriate consideration for each of the transactions listed and was not disadvantaged. This assessment has been made on the basis of the circumstances known at the time of the reportable transactions. There were no further reportable legal transactions, measures, or omissions in addition to those reported."

Essen, March 27, 2026

Marc-Julian Siewert

Torsten Henn

Dr. Kai Martius

Jessica Nospers

Balance sheet

(according to the German Commercial Code (HGB)) as at December 31, 2025

Assets

in euros	Note	31.12.2025	31.12.2024
A. Fixed assets			
I. Intangible assets		661,736.00	923,505.00
II. Tangible assets		7,569,783.00	7,501,278.00
III. Financial assets		76,209,700.84	89,040,595.04
Total fixed assets	1	84,441,219.84	97,465,378.04
B. Current assets			
I. Inventories	2	62,625,545.66	55,579,671.50
II. Receivables and other assets	3	106,378,441.98	86,404,294.70
III. Cash in hand and bank balances	4	82,879,356.04	53,819,380.22
Total current assets		251,883,343.68	195,803,346.42
C. Prepaid expenses and accrued income	5	30,099,118.43	24,059,251.15
Total Assets		**366,423,681.95**	**317,327,975.61**

Equity and liabilities

in euros	Note	31.12.2025	31.12.2024
A. Equity			
Subscribed capital		6,500,000.00	6,500,000.00
Nominal value of treasury shares		-30,498.00	-30,498.00
I. Issued capital		6,469,502.00	6,469,502.00
II. Capital reserves		21,656,305.42	21,656,305.42
III. Retained earnings			
Other retained earnings		116,662,774.13	109,250,451.13
IV. Net accumulated profit		16,691,315.16	17,661,740.46
Total equity	6	161,479,896.71	155,037,999.01
B. Provisions	7	46,064,797.25	37,293,050.28
C. Liabilities	8	63,498,152.20	47,046,902.25
D. Deferred income and accrued expenses	9	95,380,835.79	77,950,024.07
Total liabilities		**366,423,681.95**	**317,327,975.61**

Profit and loss statement

(according to the German Commercial Code (HGB)) for the period from 1 January 2025 to 31 December 2025

in euros	Note	01.01. - 31.12.2025	01.01. - 31.12.2024
Sales revenue	10	438,127,290.67	389,294,367.67
Increase in unfinished services, work in progress and finished goods		6,193,181.37	1,617,532.18
Other operating income	11	7,202,712.24	3,652,549.39
Cost of materials	12	-238,537,104.88	-208,304,001.65
Personnel expenses	13	-101,265,781.98	-94,788,570.02
Depreciation and amortization of intangible and tangible fixed assets	14	-3,861,893.07	-4,120,805.78
Other operating expenses	15	-42,048,312.95	-36,285,290.15
Financial result	16	-23,151,995.91	630,021.38
Income taxes	17	-18,524,984.00	-16,444,870.00
Earnings after taxes		24,133,111.49	35,250,933.02
Other taxes	17	-29,473.33	44,394.73
Net income for the year		24,103,638.16	35,295,327.75
Transfer to other retained earnings		-7,412,323.00	-17,633,587.29
Net accumulated profit	**18**	**16,691,315.16**	**17,661,740.46**

Notes

to the financial statements of secunet Security Networks Aktiengesellschaft for financial year 2025 (according to German Commercial Code (HGB))

General principles

secunet Security Networks Aktiengesellschaft in Essen, Germany (hereinafter referred to as "secunet AG" or "Company") is a large corporation within the meaning of Section 267 (3) Sentences 1 and 2 of the German Commercial Code (HGB) and is registered in the commercial register at the Essen Local Court (Reg. No. 13615).

The annual financial statements of secunet AG were prepared in accordance with the provisions of the German Commercial Code (HGB), taking into account the supplementary provisions of the German Stock Corporation Act (AktG).

The valuations as at December 31, 2024, were adopted unchanged.

The annual financial statements are prepared on the assumption that the Company will continue as a going concern.

The profit and loss statement is structured according to the total cost method.

To improve clarity and transparency, certain items in the balance sheet and the profit and loss statement are summarized and presented separately in the notes to the financial statements. In addition to the standard structure required under commercial law, the "Changes in fixed assets" table (Appendix to the Notes) was expanded to include the item "Premium reserve shares from reinsurance contracts" within the "Financial Assets" section.

Assets and liabilities are generally valued individually as at the reporting date.

Assets and liabilities are recognized in the financial statements at the time of the transfer of economic or legal ownership. Expenses and income for the financial year are included regardless of when the corresponding payments are made. All foreseeable risks and losses arising up to the reporting date are taken into account. Profits are recognized only if they have been realized by the reporting date.

Accounting and valuation methods

Recognition and valuation follow the principles listed below:

Assets

Fixed assets

Intangible and tangible fixed assets

Intangible assets acquired for consideration are capitalized at their historical cost upon acquisition and amortized systematically on a straight-line basis over their expected useful life. The useful life is between three and five years. In the event of a foreseeable permanent impairment, an impairment loss is recognized. Pursuant to the option under Section 248 (2) Sentence 1 of the German Commercial Code (HGB), development costs are not capitalized.

Under this item, goodwill acquired for consideration in the financial year 2016 is amortized linearly over a useful life of ten years in accordance with Section 253 (3) Sentence 4 of the German Commercial Code (HGB), as the expected useful life cannot be reliably estimated.

As at July 1, 2017, assets were acquired in an asset deal. The acquired assets and liabilities are recognized at fair value, and the excess purchase price is recognized as goodwill. This goodwill is amortized linearly over an average remaining useful life of nine years, as the software acquired in the asset deal is essential for a customer project with an average duration of nine years.

Tangible assets are valued at cost or, in the case of a foreseeable permanent impairment, at the lower fair value, and depreciated on a straight-line basis over their estimated useful lives. The useful life is between three and ten years. In the event of permanent impairment, intangible and tangible assets are written down to their lower fair value. If the reasons for the impairment cease to exist in subsequent years, the impairment loss is reversed up to a maximum of the amortized cost (excluding goodwill).

Fixed assets with acquisition costs below €1,000.00 (low-value assets) are divided into two groups. Since financial year 2018, assets with acquisition costs up to €250.00 are fully depreciated in the year of acquisition. Assets with acquisition costs between €250.00 (previously above €150.00) and €1,000.00 are placed in a collective item and depreciated linearly in the year of acquisition and over the following four years.

Financial assets

Shares in affiliated companies and investments are valued at acquisition cost.

Value adjustments are made to the lower fair value if permanent impairment is likely. Lower carrying amounts are retained unless the reasons for the impairment no longer exist, in which case a write-up is recognized up to a maximum of the original acquisition cost.

Loans to affiliated companies and companies with which there is an equity interest are accounted for at their nominal value.

Reinsurance contracts are measured at fair value.

Current assets

Inventories are valued at acquisition or production cost, or the lower fair value at the reporting date. Fair values are determined using a flat-rate method based on a retrospective valuation of the selling price. The production costs of unfinished services, work in progress and finished goods include, in addition to directly attributable costs, necessary material and manufacturing overheads, as well as general administrative expenses. Expenses for voluntary social benefits, company pension schemes, and interest on borrowed capital are not capitalized. The principles of loss-free valuation are observed.

The advance payments made are determined and recognized at their nominal value.

Trade goods are valued at the acquisition cost determined as a moving average or at the lower fair value.

Receivables and other assets are valued at nominal value less appropriate discounts for identifiable individual risks. General credit risk is accounted for by means of a general loss provision of 1%.

Cash in hand and bank balances are valued at nominal value.

Prepaid expenses refer to expenditures incurred before the reporting date, insofar as they represent expenses for a specific period after the reporting date.

Liabilities

Equity is disclosed and presented in accordance with Section 272 of the German Commercial Code (HGB).

Provisions

The provisions for pensions and similar obligations were determined according to an actuary's report based on the projected unit credit method using the 2018 G mortality tables by Prof. Dr. Klaus Heubeck. For the valuation, an actuarial interest rate of 2.07% (previous year: 1.93%) was applied, which, in accordance with the provisions of Section 253 (2) Sentence 2 of the German Commercial Code (HGB) was derived in December 2025 from the average market interest rate of the past ten years (previous year: ten) with an assumed remaining term of 15 years (previous year: 15), projected to December 31, 2025.

Applying an average market interest rate of 2.22% (previous year: 1.97%) published by Deutsche Bundesbank for the past seven financial years would lead to a liability of €7,622,795.00 as at December 31, 2025. The difference between this amount and the pension provisions, valued using an average market interest rate of 2.07% for the past ten financial years, amounts to €185,089.00 as at December 31, 2025 (previous year: €55,015.00); this amount must be taken into account when determining the amount blocked for distribution purposes (Section 253 (6) Sentence 2 of the German Commercial Code).

The effects of the change in the discount rate on earnings are recognized in the financial result. Furthermore, the valuation of direct pension obligations is based on the assumption of an increase in eligible remuneration of 3.0% (previous year: 3.0%), an increase in the adjustment of current pensions of 2.0% (previous year: 2.0%), and an average fluctuation of 6.0% (previous year: 6.0%).

According to the valuation requirements of Section 253 (1) Sentence 2 of the German Commercial Code (HGB), pension provisions are to be recognized at their settlement value since 2010.

Other provisions take into account all identifiable risks and uncertain liabilities and are recognized at the settlement amount required according to sound business judgment. Future price and cost increases are taken into account if there is sufficient objective evidence that they will occur. Provisions with a remaining term of more than one year are discounted using the average market interest rate of the past seven financial years, as determined and published by Deutsche Bundesbank. The settlement value of the warranty provision is determined based on a historical loss ratio of 7.6%, which is applied to the items in the warranty period.

Liabilities

Liabilities are recorded at their settlement value.

Income received before the reporting date, which represents income for a specific period after that date, is shown under the deferred income item.

Assets and liabilities denominated in foreign currency are translated at the time of initial valuation using the prevailing spot exchange rate.

Assets and liabilities denominated in foreign currency are translated at the spot exchange rate at the time of initial recognition. Subsequently, assets and liabilities in foreign currency with a remaining term of up to one year are measured using the spot exchange rate on the reporting date. For remaining terms of more than one year, the realization principle (Section 252 (1) No. 4 Sentence 2 of the German Commercial Code (HGB)) and the acquisition cost principle (Section 253 (1) Sentence 1 of the HGB) are observed.

Deferred taxes

The following table shows the asset and liability balances at secunet AG.

in euros	Assets	Liabilities
Fixed assets	13,743.00	0.00
Financial assets	0.00	-193,835.00
Goodwill	102,296.00	0.00
Provisions for pensions	1,280,391.00	0.00
Other provisions	695,929.00	0.00
Total	**2,092,359.00**	**-193,835.00**

Pursuant to the option under Section 274 (1) Sentence 3 of the German Commercial Code (HGB), deferred taxes assets and liabilities are presented on a net basis. The valuation of deferred taxes is based on a tax rate of 15.82% for trade tax and on tax rates between 15.83% and 10.55% for corporate tax, including the solidarity surcharge, depending on the timing of the expected reversal of the underlying temporary differences. Using the option under Section 274 (1) Sentence 2 of the HGB, deferred tax assets are not shown in the balance sheet.

Profit and loss statement

Sales revenue is recognized when the service has been rendered or the risk associated with the products sold has transferred to the customer. Services are generally billed based on hours worked. In mixed transactions, the recognition criteria must be applied separately for each partial service. In project-based business, the satisfaction of performance obligations is generally defined by acceptance protocols.

Sales revenue is recorded less value-added tax and any discounts when the delivery or service has been made and the significant risks and opportunities associated with ownership have been transferred.

Notes to the balance sheet and the profit and loss statement

1. Fixed assets

The breakdown of and changes in secunet AG's fixed assets can be found in the Changes in fixed assets table, which is attached as an appendix to the Notes.

The shareholdings as at the reporting date are as follows:

Company	Registered office	Shareholding	Equity as at December 31, 2025	Net income for 2025
secunet International GmbH	Eat	100%	€2,239 k	€4,890 k
stashcat GmbH	Hanover	100%	€-3,123 k	€-697 k
SysEleven GmbH	Berlin	100%	€-7,619 k	€-10,192 k

The previously consolidated subsidiary secustack GmbH was fully liquidated and deconsolidated in the current financial year. Its removal from the commercial register has not yet taken place.

secunet Inc., Austin, Texas/USA, 100% shareholding: equity and annual results are not disclosed due to the company's minor importance.

finally safe GmbH was renamed secunet International GmbH during the financial year. At the same time, its registered office was relocated from Essen to Munich. secunet International GmbH is a wholly owned subsidiary of secunet AG. As part of internal restructuring measures, the shares in secunet International GmbH & Co. KG (SIG) and secunet International GmbH (SIM) were contributed to secunet International GmbH. SIM was merged into secunet International GmbH in accordance with Section 2 of the German Transformation Act (UmwG). SIG was thereby absorbed by secunet International GmbH.

2. Inventories

in euros	31.12.2025	31.12.2024
Unfinished services	3,983,746.02	3,257,615.75
Work in progress	5,394,790.61	792,165.75
Finished goods	934,175.25	69,749.01
Trade goods	52,013,092.35	50,288,893.49
Advance payments	299,741.43	1,171,247.50
Total	**62,625,545.66**	**55,579,671.50**

The increase in trade goods at the reporting date is attributable to efforts to ensure short-term to medium-term delivery capability in the product business.

3. Receivables and other assets

in euros	31.12.2025	31.12.2024
Trade receivables	87,719,898.20	77,250,170.63
Receivables from affiliated companies	17,550,587.57	7,304,055.67
of which trade receivables	17,550,587.57	7,304,055.67
Other assets	1,107,956.21	1,850,068.40
Total	**106,378,441.98**	**86,404,294.70**

The remaining term for all other receivables and other assets is, as in the previous year, up to one year.

4. Cash in hand and bank balances

Liquid assets comprise cash and bank balances totaling €82,879,356.04 (previous year: €53,819,380.22).

5. Prepaid expenses and accrued income

Prepaid expenses include accruals totaling €30,099,118.43 (previous year: €24,059,251.15). These refer primarily to short-term and long-term advance payments for product services sold within the scope of customer projects.

6. Equity

The share capital amounts to €6,500,000.00. It is divided into 6,500,000 no-par-value bearer shares.

As at the reporting date, the Company continues to hold a total of 30,498 treasury shares (previous year: 30,498 shares). This corresponds to a notional value of 0.469% or €30,498 of the share capital (previous year: 0.469%). The nominal value of the treasury shares was openly offset against the share capital.

The treasury shares were acquired at their nominal value as part of a share option program for secunet employees between 2001 and 2002.

The Annual General Meeting of May 28, 2025, resolved to use the net accumulated profit for financial year 2024, amounting to €17,661,740.46, for the distribution of a dividend. A distribution of €2.73 per share (6,469,502 shares) was made starting on June 3, 2025, totaling €17,661,740.46.

Of net income for 2025 amounting to €24,103,638.16, €7,412,323.00 (= 30.75%) will be allocated to other retained earnings in accordance with Section 58 (2) Sentence 1 of the German Stock Corporation Act (AktG).

Net accumulated profit as at December 31, 2025, amounts to €16,691,315.16 (previous year: €17,661,740.46).

The majority shareholder, Giesecke+Devrient GmbH, Munich, holds a stake of 75.12% in secunet AG.

7. Provisions

in euros	31.12.2025	31.12.2024
Provisions for pensions and similar obligations	7,807,884.00	8,117,850.00
Tax provisions	3,207,752.22	589,703.00
Other provisions	35,049,161.03	28,585,497.28
Total	**46,064,797.25**	**37,293,050.28**

A breakdown of other provisions is shown in the table below:

in euros	31.12.2025	31.12.2024
Non-current provisions		
Provisions for anniversary bonuses	454,641.00	485,304.00
Non-current provision for share-based remuneration	3,519,449.00	1,585,569.00
Asset retirement and maintenance measures	526,634.95	504,357.07
Current provisions		
Annual employee bonuses	16,693,330.32	16,947,970.28
Commissions	2,483,992.85	1,200,915.75
Warranties	1,487,000.00	992,000.00
Outstanding incoming invoices	1,608,771.37	1,371,914.20
Accrued holidays	2,876,375.00	2,648,916.00
Deferred costs	1,270,000.00	0.00
Accounting and auditing costs	222,875.00	282,820.00
Current provision for share-based remuneration	229,326.68	235,650.72
Employers' liability insurance contributions	56,537.65	235,105.28
Other	3,620,227.21	2,094,974.98
Total	**35,049,161.03**	**28,585,497.28**

The provision for commissions includes payments to be made for financial year 2025 for the sale of SINA licenses, Elster sticks and connectors.

The provisions for warranties amount to €1,487,000.00 and relate to a provision for obligations arising from a three-year warranty commitment on certain SINA Core modules.

The provision for asset retirement and maintenance measures essentially includes dismantling and maintenance measures to be carried out by the Company for leased properties in Dresden, Essen, Munich, and Hanover.

8. Liabilities

in euros	31.12.2025	31.12.2024
Advance payments received on orders	445,576.10	930,298.42
Trade accounts payable	46,685,647.27	37,915,249.81
Liabilities to affiliated companies	2,131,569.70	184,960.55
of which trade payables	339,489.53	184,960.55
Other liabilities	14,235,359.13	8,016,393.47
of which taxes	14,129,454.08	7,662,124.25
of which relating to social security	10,440.34	6,712.83
Total	**63,498,152.20**	**47,046,902.25**

Liabilities have increased significantly compared to the previous year. This is primarily due to an increase in material purchases in the fourth quarter to handle the increased order volume.

Maturities

Type of liabilities (in euros)	up to one year 2025	of more than one year 2025	of which more than five years2025	up to one year previous year	of more than one year previous year	of which more than five years previous year
Advance payments received on orders	445,576.10	0.00	0.00	930,298.42	0.00	0.00
Trade accounts payable	46,685,647.27	0.00	0.00	37,915,249.81	0.00	0.00
Liabilities to affiliated companies	2,131,569.70	0.00	0.00	184,960.55	0.00	0.00
of which trade receivables	339,489.53	0.00	0.00	184,960.55	0.00	0.00
of which taxes	14,235,359.13	0.00	0.00	8,016,393.47	0.00	0.00
of which relating to social security	14,129,454.08	0.00	0.00	7,662,124.25	0.00	0.00
Total	10,440.34	0.00	0.00	6,712.73	0.00	0.00
Gesamt	**63,498,152.20**	**0.00**	**0.00**	**47,046,902.25**	**0.00**	**0.00**

9. Deferred income and accrued expenses

Deferred income and accrued expenses include deferred income amounting to €95,380,835.79 (previous year: €77,950,024.07). This relates increasingly to income from services rendered after the reporting date for the growing support business.

10. Sales revenue

The sales revenue was generated in the following regions:

in euros	2025	2024
Domestic	422,622,220.42	369,876,051.50
Abroad	15,505,070.25	19,418,316.17
Total	**438,127,290.67**	**389,294,367.67**

They are divided among the segments as follows:

in euros	2025	2024
Public	391,455,997.23	352,386,263.38
Business	46,671,293.44	36,908,104.29
Total	**438,127,290.67**	**389,294,367.67**

11. Other operating income

Other operating income of €7,202,712.24 mainly includes public project grants (€2,677,699.77), reimbursements for damages (€1,005.80), income from the reversal of provisions (€3,249,244.78), actuarial income from the adjustment of the old-age and survivor insurance premium reserve (€197,731.78) and other income (€1,077,033.11).

The income from currency translation amounts to €74,513.43 (previous year: €28,585.42).

Of the other operating income, €3,249,244.78 (45.11%) (previous year: €1,391,519.25) is non-recurring and results from the reversal of provisions.

12. Cost of materials

in euros	2025	2024
Cost of purchased goods	213,133,514.88	182,172,438.92
Cost of purchased services	25,403,590.00	26,131,562.73
Total	**238,537,104.88**	**208,304,001.65**

13. Personnel expenses

in euros	2025	2024
Wages and salaries	87,183,604.16	82,165,836.29
Social security contributions	13,969,353.34	12,463,814.13
Expenses for retirement pensions	-57,082.67	-14,476.94
Expenses for support	169,907.15	173,396.54
Total	**101,265,781.98**	**94,788,570.02**

14. Depreciation and amortization of intangible and tangible fixed assets

Depreciation and amortization are broken down by individual item in the Changes in fixed assets table (see appendix to the Notes). In the reporting year, an impairment of €17,400,000.00 was recorded on the shares in SysEleven GmbH, Berlin.

15. Other operating expenses

in euros	2025	2024
secunet Group services	3,964,266.50	4,136,469.37
Occupancy costs	6,254,433.19	6,422,990.43
Auditing, consultancy and legal costs	2,399,695.78	2,266,597.27
Travel expenses	3,492,355.16	3,213,811.40
Sales commissions	3,208,172.52	1,764,079.04
Addition to other provisions	2,293,304.45	978,105.75
Advertising costs	2,708,020.96	2,612,370.14
Ancillary personnel expenses	3,563,589.59	1,566,745.38
Communication costs	2,627,062.48	2,258,735.65
Vehicle costs	1,505,317.59	1,368,144.05
Maintenance costs	1,704,028.32	1,703,338.88
Other third-party services	587,658.97	1,599,322.86
Entertainment and representation	394,523.17	456,308.70
Insurance premiums	640,578.63	531,918.72
Fees	354,132.23	387,296.59
Licenses and concessions	2,970,708.28	2,462,090.98
Extraordinary items arising from the BilMoG revaluation of pension provisions	0.00	49,763.00
Other costs	3,380,465.13	2,507,201.94
Total	**42,048,312.95**	**36,285,290.15**

Expenses related to currency translation amounted to €227,122.36 (previous year: €112,479.28).

16. Financial result

in euros	2025	2024
Income from investments	103.857,46	0.00
Other interest and similar income	1,237,017.50	1,146,284.89
of which from affiliated companies	597,804.34	376,472.91
Depreciation of financial assets - all affiliated companies	-17,400,000.00	0.00
Write-ups of financial assets - all affiliated companies	3,111,960.31	0.00
Expenses from loss absorption	-10,192,080.17	0.00
Interest and similar expenses	-12,751.01	-516,263.51
of which from interest accrued during the year	-10,389.43	-91,676.37
Total	**-23,151,995.91**	**630,021.38**

In the reporting year, a write-down of €17,400,000 was made on the shares in SysEleven GmbH, Berlin.

As part of the Group's internal restructuring measures, the shares in secunet International GmbH (formerly finally safe GmbH) were added back in the amount of €3,111,960.31.

Income from investments includes a liquidation surplus from the winding-up of the investment in secustack GmbH, Dresden, amounting to €103,857.46 (previous year: €0.00).

17. Taxes

in euros	2025	2024
Income taxes	18,524,984.00	16,444,870.00
Other taxes	29,473.33	-44,394.73
Total	**18,554,457.33**	**16,400,475.27**

The income taxes relate predominantly to financial year 2025. Expenses amounting to €15,489.97 are not related to the accounting period.

18. Appropriation of net accumulated profit

Proposal for the appropriation of distributable earnings

From the net accumulated profit of €17,661,740.46 reported for financial year 2024, dividends of €2.73 per share, totaling €17,661,740.46, were distributed in financial year 2025 in accordance with the resolution of the Annual General Meeting of May 28, 2025.

The annual financial statements of secunet AG for financial year 2025 that are prepared in accordance with German commercial law show net income of €24,103,638.16. Of this, €7,412,323.00 (30.75%) is allocated to other retained earnings in accordance with Section 58 (2) Sentence 1 of the German Stock Corporation Act (AktG). This results in net accumulated profit of €16,691,315.16.

The Management Board proposes to the Annual General Meeting that a regular dividend of €2.58 per dividend-bearing share (corresponding to a distribution of approximately 50% of consolidated net income for the year), totaling €16,691,315.16, be distributed on the dividend-bearing share capital of €6,469,502.00. The total number of treasury shares, 30,498, was deducted in determining the dividend-bearing share capital.

in euros	2025
Net accumulated profit as at Jan 1, 2025	17,661,740.46
Dividend payment in 2025	-17,661,740.46
Net income for 2025	24,103,638.16
Allocation to other retained earnings	-7,412,323.00
Net accumulated profit as at December 31, 2025	16,691,315.16
Proposal for the appropriation of distributable earnings	
Dividend payment in 2026	-16,691,315.16
Carryforward	**0.00**

Other disclosures

Employees

The average headcount over the year was 925 (previous year: 869). Together with 105 temporary workers (previous year: 116), this takes the headcount up to 1,030 (previous year: 985), excluding Management Board members.

Other financial liabilities

The total amount of other financial liabilities was €16,890,827.04 as at the reporting date. This primarily comprises the nominal amount of liabilities arising from office leases and company car leases; of these, €5,237,092.13 are due within one year and €11,653,734.91 within a period of more than one and up to five years. There are no liabilities due after more than five years. Liabilities to affiliated companies amount to €85,931.52 and are due within one year.

A profit transfer agreement is in place between secunet Security Networks AG, Essen, and SysEleven GmbH, Berlin. Under this agreement, secunet is obligated to compensate SysEleven GmbH for any annual loss in accordance with Section 302 of the German Stock Corporation Act (AktG). The agreement has a minimum term of five years.

Purchase commitments

As at December 31, 2025, there are outstanding liabilities from orders for goods and services amounting to €48,836,634.54.

The total amount of payments required for the aforementioned commitments as at December 31, 2025, breaks down over the respective years as follows:

in euros	
2025	6,048,313.94
2026	40,080,431.79
2027	526,744.10
2028	2,178,654.71
Thereafter	2,490.00
Total	**48,836,634.54**

Contingent liabilities

The Company has liabilities amounting to €4,652.00 (previous year: €3,531.00) arising from a debt assumption and indemnification agreement with secunet International GmbH, Essen, regarding the secured direct commitments (pension, anniversary and death benefit obligations) to employees, which were transferred to the respective company as part of the transfer of business pursuant to Section 613a of the German Civil Code (BGB) effective January 1, 2018.

Due to the current economic situation of the subsidiary, no claims are expected.

A profit transfer agreement has been in place between secunet AG and SysEleven GmbH since financial year 2025.

Group affiliation

The Company is affiliated with MC Familiengesellschaft mbH, Munich, via Giesecke+Devrient GmbH, Munich, which prepares the consolidated financial statements for the largest group of companies. Furthermore, the Company is included in the consolidated financial statements of Giesecke+Devrient GmbH, Munich. Giesecke+Devrient GmbH prepares the consolidated financial statements for the smallest group of companies. The consolidated financial statements are published in the commercial register.

Auditor's fees

The total fee charged by the Company's auditor is broken down in the corresponding item of the consolidated financial statements of secunet Security Networks AG into audit services and other assurance services.

For secunet Security Networks AG and the companies it controls, other assurance services were provided primarily for services related to audits of the internal control and risk management system, the audit of the non-financial statement, and the review of the Management Board's remuneration report.

Other

The total remuneration of the active members of the Management Board pursuant to Section 285 No. 9 of the German Commercial Code (HGB) amounted to €3,341,751.00 for their activities in the reporting year (previous year: €3,041,358.15). This includes basic remuneration, fringe benefits and benefits in kind, short-term variable remuneration, and the fair value at the time of allocation of long-term variable remuneration (PSP I tranche 2025-2028 and PSP II tranche 2024-2027).

For long-term variable remuneration, provisional virtual shares were granted under the PSP I tranches 2022-2025, 2023-2026, 2024-2027, and 2025-2028, with fair values at the time of allocation amounting to €373,669.66, €309,421.29, €226,826.85, and €521,169.06, respectively. For the PSP II tranche 2024-2027, the total fair value at the time of allocation amounted to €1,020,345.96.

A provision of €1,101,279.75 was made for short-term variable remuneration during the financial year. The payment is based on the achievement of targets set by the Supervisory Board under the applicable Management Board remuneration system and is expected to be made in April 2025. The determination is based equally on the financial performance criteria of EBITDA and sales revenue.

As of the reporting date, liabilities to former members of the Management Board arising from pension commitments amount to €3,341,751.00 (previous year: €2,532,749.00).

Pension benefits totaling €50,618.00 (previous year: €50,618.00) were paid to former members of the Management Board.

Former members of the Management Board received fees totaling €11,558.00 (previous year: €18,611.00) under consultancy contracts.

The Supervisory Board's remuneration amounted to €241,073.89 in the reporting year (previous year: €142,500.00). In addition, the employee representatives on the Supervisory Board, who are employees of the Group, received salaries in accordance with their employment contracts. The remuneration was commensurate with the functions and responsibilities performed within the Group.

As of the reporting date, members of the Management Board held 1,000 shares (previous year: 1,000 shares) in the Company.

As of the reporting date, the members of the Supervisory Board held no shares in the Company.

The Management Board and the Supervisory Board of secunet AG have issued the declaration required under Section 161 of the German Stock Corporation Act (AktG). This declaration is permanently available to shareholders on the Company's website (www.secunet.com) under >> About us >> Investors >> Corporate Governance.

Declarations pursuant to Section 160 (1) No. 8 of the German Stock Corporation Act (AktG):

As of the reporting date 2025, voting rights in the Company exist. The following information is based on the disclosures made by the notifying parties pursuant to Section 33 (1) of the German Securities Trading Act (WpHG).

October 11, 2012: Publication of voting right notification pursuant to Section 21 (1) of the German Securities Trading Act (WpHG old version)

MC Familiengesellschaft mbH, headquartered in Tutzing, Germany, notified us on October 9, 2012, pursuant to Section 21 (1) of the German Securities Trading Act (WpHG), that the voting rights of MC Familiengesellschaft mbH in secunet Security Networks AG, Essen, Germany, ISIN: DE0007276503, WKN: 727650, exceeded the thresholds of 3%, 5%, 10%, 15%, 20%, 25%, 30%, 50% and 75% of the voting rights on October 8, 2012, and amounted to 79.43% (corresponding to 5,163,102 voting rights) on that day.

Of these, 78.96% (corresponding to 5,132,604 voting rights) are attributable to MC Familiengesellschaft mbH pursuant to Section 22 (1) Sentence 1 No. 1 of the German Securities Trading Act (WpHG) via Giesecke+Devrient Gesellschaft mit beschränkter Haftung, Munich, and 0.47% (corresponding to 30,498 voting rights) via secunet Security Networks AG, Essen.

February 12, 2009: Publication of voting right notification pursuant to Section 21 (1) of the German Securities Trading Act (WpHG old version)

Giesecke & Devrient Holding GmbH, Munich, Germany, notified us on February 10, 2009, pursuant to Section 21 (1) of the German Securities Trading Act (WpHG), that its voting rights in secunet Security Networks AG, Kronprinzenstraße 30, 45128 Essen, Germany, ISIN: DE0007276503, exceeded the thresholds of 5%, 10%, 25%, 50% and 75% on November 30, 2006, and amounted to 76.38% (corresponding to 4,964,958 voting rights) on that date.

Of these, 50% + 1 share (corresponding to 3,250,001 voting rights) are attributable to Giesecke & Devrient Holding GmbH via Giesecke & Devrient GmbH, pursuant to Section 22 (1) Sentence 1 No. 1 of the German Securities Trading Act (WpHG) Munich, and 26.38% (corresponding to 1,714,957 voting rights) via RWTÜV AG, Essen pursuant to Section 22 (2) of the German Securities Trading Act (WpHG).

Corporate bodies

Management Board

- Axel Deininger, Dipl.-Wirtschaftsingenieur (Industrial Engineer), Chairman of the Board / CEO (until May 20, 2025)
- Marc-Julian Siewert, Chairman of the Board / CEO (since July 1, 2025)
- Dipl.-Ing. Torsten Henn, Member of the Board / COO
- Dr. Kai Martius, Member of the Board / CTO
- Jessica Nospers, Dipl.-Kauffrau (Business Administration Graduate), Chief Financial Officer / CFO

Supervisory Board

- **Dr. Ralf Wintergerst, Baldham**
  Chairman
  Chairman of the Management Board and CEO of Giesecke+Devrient GmbH, Munich

  Other memberships on supervisory boards/control bodies:
  - Veridos GmbH (Chairman)
  - Netcetera AG, Zurich/Switzerland

- **Dr. oec. Peter Zattler, Grünwald**
  Member of the Supervisory Board
  No other memberships on supervisory boards/control bodies.

- **Jörg Marx, Dresden**
  Employee representative
  Computer scientist (Dipl.-Informatiker), secunet Security Networks AG, Essen, No other memberships on supervisory boards/control bodies.

- **Gesa-Maria Rustemeyer, Berlin**
  Eemployee representative
  Head of Legal, secunet Security Networks AG, Essen; No other memberships on supervisory boards/control bodies.

- **Jan Thyen, Munich**
  Deputy Chairman
  Member of the Management Board of Giesecke + Devrient GmbH, Munich

  Other memberships in supervisory boards/control bodies
  - Veridos GmbH, Berlin
  - Netcetera AG, Zurich/Switzerland

- **Prof. Dr.-Ing. Günter Schäfer, Berlin**
  Member of the Supervisory Board
  University Professor, Technical University, Ilmenau. No other memberships on supervisory boards/control bodies.

Events after the reporting date

Since February 28, 2026, there has been an armed conflict between the United States of America (USA) and the State of Israel on the one hand, and the Islamic Republic of Iran (Iran) on the other.

We have discussed and examined potential impacts on secunet AG. At the time of preparation of this report (mid-March 2026), no specific, material risks requiring separate assessment could be identified. However, due to the very short timeframe under consideration, a definitive evaluation is not possible.

Essen, March 27, 2026

Marc-Julian Siewert

Torsten Henn

Dr. Kai Martius

Jessica Nospers

Changes in fixed assets

secunet Security Networks AG in financial year 2025 (Appendix to the notes)

	Acquisition costs					Accumulated depreciation					Book values	
in euros	01.01.2025	Additions	Reclassifications	Disposals	31.12.2025	01.01.2025	Additions	Write-ups		Disposals31.12.2025	31.12.2025	31.12.2024
A. Intangible fixed assets												
Acquired concessions, industrial property rights and similar rights and assets, and licenses to such rights	120,000.00	0.00	0.00	-120,000.00	0.00	120,000.00	0.00	0.00	-120,000.00	0.00	0.00	0.00
Acquired software	4,665,137.27	179,889.50	480,795.00	-574,424.79	4,751,396.98	4,363,418.27	326,634.50	0.00	-551,020.79	4,139,031.98	612,365.00	301,719.00
Goodwill	3,795,966.00	0.00	0.00	0.00	3,795,966.00	3,654,975.00	91,620.00	0.00	0.00	3,746,595.00	49,371.00	140,991.00
Intangible assets under	480,795.00	0.00	-480,795.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	480,795.00
Intangible fixed assets, total	9,061,898.27	179,889.50	0.00	-694,424.79	8,547,362.98	8,138,393.27	418,254.50	0.00	-671,020.79	7,885,626.98	661,736.00	923,505.00
B. Tangible fixed assets												
Other equipment, plant and office equipment	29,464,182.28	3,493,775.57	0.00	-1,074,862.64	31,883,095.21	21,962,904.28	3,443,638.57	0.00	-998,114.64	24,408,428.21	7,474,667.00	7,501,278.00
Assets under construction	0.00	95,116.00	0.00	0.00	95,116.00	0.00	0.00	0.00	0.00	0.00	95,116.00	0.00
Tangible fixed assets, total	29,464,182.28	3,588,891.57	0.00	-1,074,862.64	31,978,211.21	21,962,904.28	3,443,638.57	0.00	-998,114.64	24,408,428.21	7,569,783.00	7,501,278.00
C. Financial assets												
Shares in affiliated companies	73,601,761.11	136,517.49	0.00	0.00	73,738,278.60	3,736,907.07	17,400,000.00	-3,111,960.31	0.00	18,024,946.76	55,713,331.84	69,864,854.04
Shares in affiliated partnerships	108,231.00	0.00	0.00	-108,231.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	108,231.00
Loans to affiliated companies	12,413,550.26	1,500,000.00	0.00	-613,550.26	13,300,000.00	613,550.26	0.00	0.00	-613,550.26	0.00	13,300,000.00	11,800,000.00
Premium reserve shares from reinsurance contracts	7,267,510.00	125,556.00	0.00	-196,697.00	7,196,369.00	0.00	0.00	0.00	0.00	0.00	7,196,369.00	7,267,510.00
Financial assets, total	93,391,052.37	1,762,073.49	0.00	-918,478.26	94,234,647.60	4,350,457.33	17,400,000.00	-3,111,960.31	-613,550.26	18,024,946.76	76,209,700.84	89,040,595.04
Total fixed assets	**131,917,132.92**	**5,530,854.56**	**0.00**	**-2,687,765.69**	**134,760,221.79**	**34,451,754.88**	**21,261,893.07**	**-3,111,960.31**	**-2,282,685.69**	**50,319,001.95**	**84,441,219.84**	**97,465,378.04**

Note: This is a convenience translation of the German original. Solely the original text in German is authoritative.

Independent Auditor's Report

To secunet Security Networks Aktiengesellschaft, Essen

Report on the Audit of the Annual Financial Statements and the Combined Management Report

Audit Opinions

We have audited the annual financial statements of secunet Security Networks Aktiengesellschaft , Essen, which comprise the balance sheet as at 31 December 2025, the statement of profit or loss for the financial year from 1 January 2025 to 31 December 2025 and notes to the annual financial statements, including the presentation of the recognition and measurement policies.

In addition, we have audited the combined management report (report on the position of the company and of the group) of secunet Security Networks Aktiengesellschaft for the financial year from 1 January 2025 to 31 December 2025. In accordance with the German legal requirements, we have not audited the content of the parts of the combined management report listed in section "OTHER INFORMATION".

In our opinion, on the basis of the knowledge obtained in the audit,

- the accompanying annual financial statements comply, in all material respects, with the requirements of German commercial law applicable to business corporations and give a true and fair view of the assets, liabilities and financial position of the company as at 31 December 2025 and of its financial performance for the financial year from 1 January 2025 to 31 December 2025 in compliance with German Legally Required Accounting Principles, and
- the accompanying combined management report as a whole provides an appropriate view of the company's position. In all material respects, this combined management report is consistent with the annual financial statements, complies with German legal requirements and appropriately presents the opportunities and risks of future development. Our audit opinion on the combined management report does not cover the content of those parts of the combined management report listed in section "OTHER INFORMATION".

Pursuant to § 322 (3) sentence 1 HGB (German Commercial Code), we declare that our audit has not led to any reservations relating to the legal compliance of the annual financial statements and of the combined management report.

Basis for Audit Opinions

We conducted our audit of the annual financial statements and of the combined management report in accordance with § 317 HGB and the EU Audit Regulation (No. 537/2014, referred to subsequently as "EU Audit Regulation") and in compliance with German Generally Accepted Standards for Financial Statement Audits promulgated by the Institut der Wirtschaftsprüfer [Institute of Public Auditors in Germany] (IDW). Our responsibilities under those requirements and principles are further described in the "AUDITOR'S RESPONSIBILITIES FOR THE AUDIT OF THE ANNUAL FINANCIAL STATEMENTS AND OF THE COMBINED MANAGEMENT REPORT" section of our auditor's report. We are independent of the company in accordance with the requirements of European law and German commercial and professional law, and we have fulfilled our other German professional responsibilities in accordance with these requirements.

In addition, in accordance with Article 10 (2) letter (f) of the EU Audit Regulation, we declare that we have not provided non-audit services prohibited under Article 5 (1) of the EU Audit Regulation.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinions on the annual financial statements and on the combined management report.

Key Audit Matters in the Audit of the Annual Financial Statements

Key audit matters are those matters that, in our professional judgment, were of most significance in our audit of the annual financial statements for the financial year from 1 January 2025 to 31 December 2025. These matters were addressed in the context of our audit of the annual financial statements as a whole, and in forming our audit opinion thereon; we do not provide a separate audit opinion on these matters.

We have identified the following matters as key audit matters to be disclosed in our auditor's report:

- 1. Revenue recognition
- 2. Goodwill Impairment

1. Revenue Recognition

Matter

The annual financial statements of secunet Security Networks Aktiengesellschaft report revenue of EUR 438 million in the income statement. On the one hand, secunet Security Networks Aktiengesellschaft generates revenue from the sale of hardware products and software licenses, which it recognizes when the service has been rendered and the risk has passed to the customer. If additional services are agreed upon with the customer at the same time, particularly for maintenance, updates, and extended warranty commitments, the revenue recognition criteria are applied individually to each component.

Furthermore, secunet Security Networks Aktiengesellschaft recognizes revenue from the provision of specialized services for consulting on the implementation of comprehensive IT security solutions as well as for software development, primarily based on the hours worked as of the reporting date or on the basis of the stage of completion.

Due to the customer structure, which consists predominantly of public-clients such as government agencies, ministries, and organizations in the defense sector, the number of orders and, accordingly, the order and service volume in the fourth quarter of the fiscal year is comparatively higher than in the other quarters.

Given the high number of business transactions at the end of the fiscal year, combined with the various contractual agreements, there is a significant risk that revenue for the past fiscal year may not be recognized in the correct period. Against this background, this matter was of particular importance for our audit.

The Company's disclosures regarding revenue are included in the notes under the section "Accounting and Valuation Methods" and section 10, "Revenue."

Auditor's Response and Observations

As part of our audit, including through the use of IT-assisted audit techniques, we assessed, among other things, the adequacy and effectiveness of the Company's internal control system with respect to the complete and accurate recognition and timely revenue recognition. In addition, we obtained an understanding of the underlying contractual agreements and evaluated them with respect to revenue recognition. To assess revenue recognition, we reviewed and evaluated the relevant contractual documents and evaluated them, and focused on comparing the invoices for sales selected on a sample basis that were recognized in December 2025 and January 2026 with the associated purchase orders, contracts, external delivery notes, acceptance reports, and time sheets.

In addition, we obtained third-party confirmations for trade receivables based on a sample selection. Where we did not receive responses regarding the requested revenue transactions, we verified them through alternative audit procedures, in particular by reconciling the revenue with the aforementioned external documents.

Overall, we were satisfied that the systems and processes established by the legal representatives, as well as the controls in place, are adequate to ensure revenue recognition in the appropriate period.

2. Goodwill Impairment

Matter

In the annual financial statements of secunet Security Networks Aktiengesellschaft (hereinafter "secunet AG"), investments in affiliated companies (EUR 55,713 thousand; prior year: EUR 69,973 thousand) are reported under financial assets, which together account for 15% of total assets.

The assessment of the recoverability of investments in affiliated companies involves judgment and is primarily based on forecasts of the future earnings situation of the subsidiaries. These forecasts are based on a three-year plan and depend to a large extent on the estimation of future cash inflows, taking into account growth rates and the cost of capital.

Due to the material significance of the investments in affiliated companies for the financial statements of secunet AG and the considerable uncertainties associated with their valuation, this constitutes a particularly important audit matter.

The disclosures by secunet AG regarding investments in affiliated companies are included in the §s "Accounting and Valuation Methods" and "Notes to the Balance Sheet" of the Notes to the Financial Statements.

Auditor's Response and Observations

As part of our audit, we assessed the appropriateness of the key assumptions and judgmental parameters, as well as the calculation method used in the impairment tests, with the involvement of our valuation specialists. We reviewed the judgments and estimates made by the legal representatives of secunet AG in assessing the recoverability of the investments in affiliated companies and, in doing so, formed an opinion regarding the appropriate derivation of the basis for the discretionary decisions and estimates. First, we gained an understanding of the planning methodology and the planning process and reviewed the available plans of the subsidiaries, which had been approved by the shareholders' meeting, for consistency, taking into account the economic market environment. In doing so, we also assessed the appropriateness of the valuation methods used for the impairment tests of the investments in affiliated companies, which are based on the use of discounted cash flow models with weighted average cost of capital.

Overall, we were satisfied that the assumptions made by the legal representatives in performing the investment valuation and the valuation parameters used are reasonable and fall within an acceptable range.

Other Information

The executive directors or the supervisory board are responsible for the other information. The other information:

- the separately published corporate governance statement pursuant to § 289f and § 315d of the German Commercial Code (HGB), to which reference is made in the section "Management and Control – Reference to the Corporate Governance Statement pursuant to § 289f and § 315d of the German Commercial Code (HGB)" of the consolidated management report
- the separately published compensation report within the meaning of § 162 of the German Stock Corporation Act (AktG), to which reference is made in the section "Management System and Key Performance Indicators" under the financial key performance indicators of the combined management report.
- the information contained in the combined management report that is not part of the management report and is marked as unaudited. This includes the reporting contained in the section "Risk Management and Internal Control System," subsection "Statement on the Adequacy and Effectiveness of Governance Systems"
- the remaining parts of the annual report, with the exception of the audited financial statements and the consolidated management report, as well as our audit opinion

Our audit opinions on the annual financial statements and on the combined management report do not cover the other information, and consequently we do not express an audit opinion or any other form of assurance conclusion thereon.

In connection with our audit, our responsibility is to read the other information and thereby acknowledge whether the other information

- is materially inconsistent with the annual financial statements, with the combined management report or our knowledge obtained in the audit, or
- otherwise appears to be materially misstated.

If, based on the work we have performed, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

Responsibilities of the Executive Directors and the Supervisory Board for the Annual Financial Statements and the Combined Management Report

The executive directors are responsible for the preparation of the annual financial statements that comply, in all material respects, with the requirements of German commercial law applicable to business corporations, and that the annual financial statements give a true and fair view of the assets, liabilities, financial position and financial performance of the company in compliance with German Legally Required Accounting Principles. In addition, the executive directors are responsible for such internal control as they, in accordance with German Legally Required Accounting Principles, have determined necessary to enable the preparation of annual financial statements that are free from material misstatement, whether due to fraud (i. e. fraudulent financial reporting and misappropriation of assets) or error.

In preparing the annual financial statements, the executive directors are responsible for assessing the company's ability to continue as a going concern. They also have the responsibility for disclosing, as applicable, matters related to going concern. In addition, they are responsible for financial reporting based on the going concern basis of accounting, provided no actual or legal circumstances conflict therewith.

Furthermore, the executive directors are responsible for the preparation of the combined management report that as a whole provides an appropriate view of the company's position and is, in all material respects, consistent with the annual financial statements, complies with German legal requirements, and appropriately presents the opportunities and risks of future development. In addition, the executive directors are responsible for such arrangements and measures (systems) as they have considered necessary to enable the preparation of a combined management report that is in accordance with the applicable German legal requirements, and to be able to provide sufficient appropriate evidence for the assertions in the combined management report.

The supervisory board is responsible for overseeing the company's financial reporting process for the preparation of the annual financial statements and of the combined management report.

Auditor's Responsibilities for the Audit of the Annual Financial Statements and of the Combined Management Report

Our objectives are to obtain reasonable assurance about whether the annual financial statements as a whole are free from material misstatement, whether due to fraud or error, and whether the combined management report as a whole provides an appropriate view of the company's position and, in all material respects, is consistent with the annual financial statements and the knowledge obtained in the audit, complies with the German legal requirements and appropriately presents the opportunities and risks of future development, as well as to issue an auditor's report that includes our audit opinions on the annual financial statements and on the combined management report.

Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with § 317 HGB and the EU Audit Regulation and in compliance with German Generally Accepted Standards for Financial Statement Audits promulgated by the Institut der Wirtschaftsprüfer (IDW) and supplementary compliance with the ISAs will always detect a material misstatement. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these annual financial statements and this combined management report.

We exercise professional judgment and maintain professional skepticism throughout the audit. We also

- identify and assess the risks of material misstatement of the annual financial statements and of the combined management report, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our audit opinions. The risk of not detecting a material misstatement resulting from fraud is higher than the risk of not detecting a material misstatement resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal controls.

- obtain an understanding of internal controls relevant to the audit of the annual financial statements and of arrangements and measures relevant to the audit of the combined management report in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an audit opinion on the effectiveness of the internal controls or these arrangements and measures of the company.

- evaluate the appropriateness of accounting policies used by the executive directors and the reasonableness of estimates made by the executive directors and related disclosures.

- conclude on the appropriateness of the executive directors' use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the company's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in the auditor's report to the related disclosures in the annual financial statements and in the combined management report or, if such disclosures are inadequate, to modify our respective audit opinions. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the company to cease to be able to continue as a going concern.

- evaluate the overall presentation, structure and content of the annual financial statements, including the disclosures, and whether the annual financial statements present the underlying transactions and events in a manner that the annual financial statements give a true and fair view of the assets, liabilities, financial position and financial performance of the company in compliance with German Legally Required Accounting Principles.

- evaluate the consistency of the combined management report with the annual financial statements, its conformity with [German] law, and the view of the company's position it provides.

- perform audit procedures on the prospective information presented by the executive directors in the combined management report. On the basis of sufficient appropriate audit evidence we evaluate, in particular, the significant assumptions used by the executive directors as a basis for the prospective information, and evaluate the proper derivation of the prospective information from these assumptions. We do not express a separate audit opinion on the prospective information and on the assumptions used as a basis. There is a substantial unavoidable risk that future events will differ materially from the prospective information.

We communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal controls that we identify during our audit.

We also provide those charged with governance with a statement that we have complied with the relevant independence requirements, and communicate with them all relationships and other matters that may reasonably be thought to bear on our independence, and, where applicable, the actions taken or safeguards applied to eliminate independence threats.

From the matters communicated with those charged with governance, we determine those matters that were of most significance in the audit of the annual financial statements of the current period and are therefore the key audit matters. We describe these matters in our auditor's report unless law or regulation precludes public disclosure about the matter.

Other Legal and Regulatory Requirements

Report on the Assurance on the Electronic Rendering of the Annual Financial Statements and the Combined Management Report, Prepared for Publication Purposes in accordance With § 317 (3a) HGB

Assurance Opinion

We have performed assurance work in accordance with § 317 (3a) HGB to obtain reasonable assurance as to whether the rendering of the annual financial statements and the combined management report (hereinafter the "ESEF documents") contained in the electronic file "secunet_AG_JA_LB_ESEF_2025_12_31.zip" and prepared for publication purposes complies in all material respects with the requirements of § 328 (1) HGB for the electronic reporting format ("ESEF format"). In accordance with German legal requirements, this assurance work extends only to the conversion of the information contained in the annual financial statements and the combined management report into the ESEF format and therefore relates neither to the information contained within these renderings nor to any other information contained in the file identified above.

In our opinion, the rendering of the annual financial statements and the combined management report contained in the electronic file identified above and prepared for publication purposes complies in all material respects with the requirements of § 328 (1) HGB for the electronic reporting format. Beyond this assurance opinion and our audit opinion on the accompanying annual financial statements and the accompanying combined management report for the financial year from 1 January 2025 to 31 December 2025 contained in the "Report on the audit of the annual financial statements and of the combined management report" above, we do not express any assurance opinion on the information contained within these renderings or on the other information contained in the file identified above.

Basis for the Assurance Opinion

We conducted our assurance work on the rendering of the annual financial statements and the combined management report contained in the file identified above in accordance with § 317 (3a) HGB and the IDW Assurance Standard: Assurance Work on the Electronic Rendering of Financial Statements and Management Reports, Prepared for Publication Purposes in Accordance with § 317 (3a) HGB (IDW AsS 410 (06.2022)).

Our responsibility in accordance therewith is further described in the "Auditor's Responsibilities for the Assurance Work on the ESEF Documents" section. Our audit firm has applied the requirements of the IDW Quality Management Standard: Requirements for Quality Management in the Audit Firm (IDW QMS 1 (09.2022)).

Responsibilities of the Executive Directors and the Supervisory Board for the ESEF Documents

The executive directors of the company are responsible for the preparation of the ESEF documents with the electronic renderings of the annual financial statements and the combined management report in accordance with § 328 (1) sentence 4 No. 1 HGB.

In addition, the executive directors of the company are responsible for such internal controls that they have considered necessary to enable the preparation of ESEF documents that are free from material intentional or unintentional non-compliance with the requirements of § 328 (1) HGB for the electronic reporting format.

The supervisory board is responsible for overseeing the process for preparing the ESEF documents as part of the financial reporting process.

Auditor's Responsibilities for the Assurance Work on the ESEF documents

Our objective is to obtain reasonable assurance about whether the ESEF documents are free from material intentional or unintentional non-compliance with the requirements of § 328 (1) HGB. We exercise professional judgment and maintain professional skepticism throughout the assurance work. We also

- identify and assess the risks of material intentional or unintentional non-compliance with the requirements of § 328 (1) HGB, design and perform assurance procedures responsive to those risks, and obtain assurance evidence that is sufficient and appropriate to provide a basis for our assurance opinion.

- obtain an understanding of internal control relevant to the assurance on the ESEF documents in order to design assurance procedures that are appropriate in the circumstances, but not for the purpose of expressing an assurance opinion on the effectiveness of these controls.

- evaluate the technical validity of the ESEF documents, i. e. whether the file containing the ESEF documents meets the requirements of the Delegated Regulation (EU) 2019/815, in the version in force at the date of the financial statements, on the technical specification for this electronic file.

- evaluate whether the ESEF documents provide an XHTML rendering with content equivalent to the audited annual financial statements and to the audited combined management report.

Further Information Pursuant to Article 10 of the EE Audit Regulation

We were elected as auditor by the annual general meeting on 25 May 2025. We were engaged by the supervisory board on 16 September 2025. We have been the auditor of the secunet Security Networks Aktiengesellschaft without interruption since the financial year 2023.

We declare that the audit opinions expressed in this auditor's report are consistent with the additional report to the audit committee pursuant to Article 11 of the EU Audit Regulation (long-form audit report).

Other Matter — Use of the Auditor's Report

Our auditor's report must always be read together with the audited annual financial statements and the audited combined management report as well as the assured ESEF documents. The annual financial statements and the combined management report converted to the ESEF format — including the versions to be published in the German Company Register — are merely electronic renderings of the audited annual financial statements and the audited combined management report and do not take their place. In particular, the ESEF report and our assurance opinion contained therein are to be used solely together with the assured ESEF documents provided in electronic form.

German Public Auditor Responsible for the Engagement

The German Public Auditor responsible for the engagement is Dr. Marcus Falk..

Essen, March 26, 2026
BDO AG Wirtschaftsprüfungsgesellschaft

signed Dr. Marcus Falk
Auditor

Responsibility statement

"To the best of our knowledge, we assure that, in accordance with the applicable accounting principles, the consolidated financial statements present a true and fair view of the Group's assets, liabilities, financial position and results of operations, and that the Group management report gives a true and fair view of the business performance, including the business results and the Group's position, together with a description of the principal opportunities and risks of the Group's expected future development."

Essen, March 27, 2026

Marc-Julian Siewert

Torsten Henn

Dr. Kai Martius

Jessica Nospers

Assurance report by the independent German public auditor on a limited assurance engagement in relation to the Group Sustainability Statement

To secunet Security Networks Aktiengesellschaft, Essen

Assurance conclusion

We have conducted a limited assurance engagement on the Group Sustainability Statement, included in section "Group Sustainability Statement" of the group management report, of secunet Security Networks Aktiengesellschaft, Essen (hereinafter referred to as "secunet" or "the Company") for the financial year from 1. January 2025 to 31. December 2025. The Group Sustainability Statement was prepared to fulfil the requirements of Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 (Corporate Sustainability Reporting Directive, CSRD) and Article 8 of Regulation (EU) 2020/852 as well as Articles 315b and 315c in conjunction with Articles 289b to 289e of the German Commercial Code (HGB) for a group non-financial statement.

References to the Group's website, contained in the Group Sustainability Statement (see appendix to this Assurance Report) are not subject to our assurance engagement.

Based on the procedures performed and the evidence obtained as part of our limited assurance engagement, nothing has come to our attention that causes us to believe that the accompanying Group Sustainability Statement, is not prepared, in all material respects, in accordance with the requirements of the CSRD and Article 8 of Regulation (EU) 2020/852, Articles 315b and 315c in conjunction with Articles 289b to 289e HGB for a combined non- financial statement and the supplementary criteria presented by the executive directors of the Company. This assurance conclusion includes that nothing has come to our attention that causes us to believe that:

- the accompanying Group Sustainability Statement does not comply, in all material respects, with the European Sustainability Reporting Standards (ESRS), including that the process carried out by the entity to identify information to be included in the Group Sustainability Statement (the materiality assessment) is not, in all material respects, in accordance with the description set out in section "ESRS 2: General Disclosures" of the Group Sustainability Statement, or

- the disclosures in the Group Sustainability Statement do not comply, in all material respects, with Article 8 of Regulation (EU) 2020/852.

We do not express an assurance conclusion on references to the Group's Website in the Group Sustainability Statement (see appendix to this Assurance Report).

Basis for the assurance conclusion and opinion

We conducted our assurance engagement in accordance with International Standard on Assurance Engagements (ISAE) 3000 (Revised): Assurance Engagements Other Than Audits or Reviews of Historical Financial Information issued by the International Auditing and Assurance Standards Board (IAASB).

The procedures in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement. Consequently, the level of assurance obtained is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed.

Our responsibilities under ISAE 3000 (Revised) are further described in the section "German Public Auditor's Responsibilities for the Assurance Engagement on the Group Sustainability Statement".

We are independent of secunet in accordance with the requirements of European law and German commercial and professional law, and we have fulfilled our other German professional responsibilities in accordance with these requirements. Our audit firm has applied the requirements for a system of quality control as set forth in the IDW Quality Management Standard issued by the Institute of Public Auditors in Germany (IDW): Requirements for Quality Management in the Audit Firm (IDW QMS 1 (09.2022)). We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our assurance conclusion and opinion.

Responsibility of the executive directors and the Supervisory Board for the Group Sustainability Statement

The executive directors are responsible for the preparation of the Group Sustainability Statement in accordance with the requirements of the CSRD and the applicable German legal and other European requirements as well as with the supplementary criteria presented by the executive directors of the Company and for designing, implementing and maintaining such internal control that they have considered necessary to enable the preparation of the Group Sustainability Statement in accordance with these requirements that is free from material misstatement, whether due to fraud (i. e., fraudulent sustainability reporting in the Group Sustainability Statement) or error.

This responsibility of the executive directors includes establishing and maintaining the materiality assessment process, selecting and applying appropriate reporting policies for preparing the Group Sustainability Statement, as well as making assumptions and estimates and ascertaining forward-looking information for individual sustainability-related disclosures.

The Supervisory Board is responsible for overseeing the process for the preparation of the Group Sustainability Statement.

Inherent limitations in the preparation of the Group Sustainability Statement

The CSRD and the applicable German legal and other European requirements contain wording and terms that are subject to considerable interpretation uncertainties and for which no authoritative, comprehensive interpretations have yet been published. As such wording and terms may be interpreted differently by regulators or courts, the legality of measurements or evaluations of sustainability matters based on these interpretations is uncertain.

These inherent limitations also affect the assurance engagement on the Group Sustainability Statement.

German public auditor's responsibilities for the assurance engagement on the Group Sustainability Statement

Our objectives are to express a limited assurance conclusion, based on the assurance engagement we have conducted, on whether any matters have come to our attention that cause us to believe that the Group Sustainability Statement, has not been prepared, in all material respects, in accordance with the CSRD, the applicable German legal and other European requirements and the supplementary criteria presented by the Company's executive directors, and to issue an assurance report that includes our assurance conclusion on the Group Sustainability Statement.

As part of an assurance engagement in accordance with ISAE 3000 (Revised), we exercise professional judgment and maintain professional skepticism. We also:

- obtain an understanding of the process used to prepare the Group Sustainability Statement, including the materiality assessment process carried out by the entity to identify the disclosures to be reported in the Group Sustainability Statement.

- identify disclosures where a material misstatement due to fraud or error is likely to arise, design and perform procedures to address these disclosures and

obtain limited assurance to support the assurance conclusion. The risk of not detecting a material misstatement resulting from fraud is higher than the risk of not detecting a material misstatement resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations or the override of internal control. In addition, the risk of not detecting a material misstatement in information obtained from sources not within entity's control (value chain information) is ordinarily higher than the risk of not detecting a material misstatement in information obtained from sources within the entity's control, as both the entity's executive directors and we as practitioners are ordinarily subject to restrictions on direct access to the sources of the value chain information.

- consider the forward-looking information, including the appropriateness of the underlying assumptions. There is a substantial unavoidable risk that future events will differ materially from the forward-looking information.

Summary of the procedures for the lmited assurance engagement by the german public auditor

A limited assurance engagement involves the performance of procedures to obtain evidence about the sustainability information. The nature, timing and extent of the selected procedures are subject to our professional judgment.

In performing our limited assurance engagement, we:

- evaluated the suitability of the criteria as a whole presented by the executive directors in the Group Sustainability Statement.
- inquired of the executive directors and relevant employees involved in the preparation of the Group Sustainability Statement about the preparation process, including the materiality assessment process carried out by the entity to identify the disclosures to be reported in the Group Sustainability Statement, and about the internal controls relating to this process.
- evaluated the reporting policies used by the executive directors to prepare the Group Sustainability Statement.
- evaluated the reasonableness of the estimates and related information provided by the executive directors. If, in accordance with the ESRS, the executive directors estimate the value chain information to be reported for a case in which the executive directors are unable to obtain the information from the value chain despite making reasonable efforts, our assurance engagement is limited to evaluating whether the executive directors have undertaken these estimates in accordance with the ESRS and assessing the reasonableness of these estimates, but does not include identifying information in the value chain that the executive directors were unable to obtain.
- performed analytical procedures and made inquiries in relation to selected information in the Group Sustainability Statement.
- considered the presentation of the information in the Group Sustainability Statement.
- considered the process for identifying taxonomy-eligible and taxonomy-aligned economic activities and the corresponding disclosures in the Group Sustainability Statement.

Restrictions on the use

We draw attention to the fact that the assurance engagement was conducted for the Company's purposes and that the assurance report is intended solely to inform the Company about the result of the assurance engagement. Consequently, it may not be suitable for any other purpose than the aforementioned. Accordingly, the assurance report is not intended to be used by third parties for making (financial) decisions based on it. Our responsibility is to the Company alone. We do not accept any responsibility to third parties. Our assurance conclusion is not modified in this respect.

Engagement terms

This engagement is based on the "Special Terms and Conditions of BDO AG Wirtschaftsprüfungsgesellschaft" dated July 1, 2025, agreed with the Company as well as the „General Engagement Terms for Wirtschaftsprüferinnen, Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften (German Public Auditors and Public Audit Firms)" dated January 1, 2024, issued by the IDW (www.bdo.de/engagement-terms-conditions).

Hamburg, March 27, 2026

BDO AG
Wirschaftsprüfungsgesellschaft

signed Fritz
German Public Auditor

signed Dr. Falk
German Public Auditor

Appendix to the assurance report: Unassured elements for the Group Sustainability Statement

References to the Group's website, contained in the Group Sustainability Statement (see appendix to this Assurance Report) were not subject to our assurance engagement. The information to which these references pertain has not been substantively audited by us.

Service

Locations

Headquarters Essen
secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen

Phone: +49 201 5454-0
Fax: +49 201 5454-1000

Berlin
secunet Security Networks AG
Alt-Moabit 96
10559 Berlin

Berlin
SysEleven GmbH
Boxhagener Straße 80
10245 Berlin

Bonn
secunet Security Networks AG
Dreizehnmorgenweg 6
53175 Bonn

Dresden
secunet Security Networks AG
Ammonstraße 74
01067 Dresden

Frankfurt
secunet Security Networks AG
Mergenthalerallee 77
65760 Eschborn

Hamburg
secunet Security Networks AG
Osterbekstraße 90 b
22083 Hamburg

Hanover
stashcat GmbH
Schiffgraben 47
30175 Hannover

Ilmenau
secunet Security Networks AG
Werner-von-Siemens-Straße 6
98693 Ilmenau

Munich
secunet Security Networks AG
Konrad-Zuse-Platz 2-12
81829 Munich

Paderborn
secunet Security Networks AG
Hauptstraße 35
33178 Borchen

Siege
secunet Security Networks AG
Weidenauer Straße 223-225
57076 Siegen

Stuttgart
secunet Security Networks AG
Neue Brücke 3
70173 Stuttgart

Training Center Dresden
secunet Security Networks AG
Ammonstraße 74
01067 Dresden

Financial calendar

March 30, 2026
Annual Report 2025

May 5, 2026
Group Quarterly Statement as at March 31, 2026

June 8, 2026
Annual General Meeting 2026

August 13, 2026
Half-Year Financial Report 2026

November 12, 2026
Group Quarterly Statement as at September 30, 2026

Legal information

Issued by
secunet Security Networks AG Security Networks AG
Kurfürstenstraße 58
45138 Essen

Phone: +49 201 54 54-0
Email: info@secunet.com
www.secunet.com

Investor Relations
Phone: +49 201 54 54-3426
Email: investor.relations@secunet.com

Press
Phone: +49 201 54 54-1234
Email: presse@secunet.com

Concept, design and setting
IR-ONE AG & Co. KG, Hamburg
www.ir-one.de

Text
secunet Security Networks AG

Notes

This annual report contains statements relating to the future development of the secunet Group as well as economic and political developments. These statements represent assessments made based on the information available to us at present. Should the underlying assumptions prove incorrect, or should further risks materialize, actual results may differ from those currently expected. We therefore cannot guarantee the accuracy of these statements.

Due to rounding, it is possible that individual figures in this annual report may not add up exactly to the stated total, and that percentages shown may not precisely reflect the absolute values to which they refer.

This annual report was published on March 30, 2026. It is available in German and English. Both versions can be downloaded from www.secunet.com. In case of doubt, the German version shall prevail.

secunet

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen

Tel.: +49 201 5454 - 0
Fax: +49 201 5454 - 1000

Email: info@secunet.com
Internet: www.secunet.com

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig