Information Security and Data Protection Policy

Adopted by the Grant Thornton Board of Directors 10 December 2024

Valid from 1 January 2025

Policy owner: Chief Information Officer

Information classification: Open

1. Introduction and purpose

Grant Thornton Sweden AB's ("Grant Thornton") Information Security and Data Protection Policy, together with the Code of Conduct, our success factors and other governing documents, shall contribute to the company's success and the achievement of its goals. The purpose of the policy is to increase quality, ensure compliance with legal requirements and underpin the company's strategy and vision by establishing principles for information security and data protection. The policy is an important part of the company's quality, risk, compliance and sustainability management.

Grant Thornton handles large amounts of information, both within the context of client activities and internally. External and internal rules on auditing, professional ethics and data protection set high standards regarding the security of both business information and personal data.

2. Scope

The policy applies to all persons working at or for Grant Thornton, including employees, trainees and (where applicable) external consultants, who are referred to as employees in the governing documents. The "Supplier Code of Conduct" applies to suppliers and other partners. Roles and responsibilities are described in an overarching way in the Grant Thornton governance framework.

Focus areas in this policy

- Roles and responsibilities relating to information security
- Roles and responsibilities relating to data protection
- Appropriate protection of information and personal data
- Internal reporting of various types of incidents relating to information security and data protection

3. General regulatory compliance

Grant Thornton shall comply with all the applicable laws of the countries and jurisdictions in which the company operates, as well as, to the extent applicable, standards and international guidelines relating to the areas covered by this policy, including standards issued by Grant Thornton International Limited ("GTIL").

Public information. May be freely shared and distributed.

4. Training, guidance and awareness-raising activities

Grant Thornton shall strive to raise awareness about the content of the policy among its employees. Training, guidance and communication activities shall be relevant and tailored to the specific roles and organisational affiliations. The effectiveness of the activities shall be monitored.

5. Information security and data protection activities at Grant Thornton

Grant Thornton's risk-based approach to information security and data protection is based on applicable data protection legislation as well as international information security standards and guidelines. The purpose is to enable us as a company to comply with relevant regulations and provide appropriate protection of the information and personal data handled in the business, and to achieve a good culture regarding information security and data protection.

Fundamental elements of information security and data protection are the existence of clear roles and responsibilities in each area, the provision of appropriate protection of information and personal data, and that various types of incidents relating to information security and data protection are reported and handled internally.

Grant Thornton shall work actively with information security activities in order to protect Grant Thornton's information assets in an appropriate manner, reduce the risk of misuse of business information and prevent IT-related disruptions that may adversely affect business activities. The protection that is implemented shall be adapted to the nature, scope and risk involved, taking into account both external and internal requirements defined in laws, regulations and internal governing documents.

Grant Thornton shall work actively with data protection activities in order to ensure an appropriate level of compliance with applicable data protection legislation and maintain appropriate organisational and technical protection for personal data that is processed. A good data protection culture is an important part of the overall information security culture.

5.1. Roles and responsibilities relating to information security

All employees have a responsibility to ensure good information security in their daily work. Within Grant Thornton, the CEO is ultimately responsible for information security and compliance with information security requirements at Grant Thornton. The operational responsibility for information security and information ownership resides with the respective Business Leader and Corporate Functions. In addition, a Chief Information Security Officer (CISO) and a system owner shall be appointed and/or defined.

5.1.1. A good information security culture

A good information security culture means that all employees shall be aware of their own particular responsibility for information security and which rules are applicable and have the ability to recognise events that could have an adverse impact on information security. By providing training and information, all employees shall be made aware of information security issues, as this underpins compliance and promotes a good information security culture.

Public information. May be freely shared and distributed.

5.2. Roles and responsibilities relating to data protection

All employees have a responsibility to maintain an appropriate level of protection for personal data that is processed in the context of their daily work. Within Grant Thornton, the Board of Directors is ultimately responsible for ensuring that personal data is processed in accordance with the applicable data protection legislation. The operational responsibility for ensuring compliance with data protection rules is linked to the information ownership, i.e. it is the responsibility of the relevant manager. Grant Thornton shall appoint a Data Protection Officer (DPO). The authority and fundamental tasks of this role are defined in the applicable data protection legislation. The DPO is not responsible for ensuring compliance with applicable data protection legislation, as that is always the responsibility of the data controller.

5.2.1. A good data protection culture

Grant Thornton shall work actively with data protection to ensure compliance with data protection regulations when personal data is processed as part of Grant Thornton's business operations. It is important that the fundamental principles regarding the processing of personal data are respected. Data protection shall form an integral part of daily business activities. By providing training and information, all employees shall be made aware of data protection issues, as this underpins a high level of protection for personal data that is processed and promotes a good data protection culture.

5.3. Appropriate protection of information and personal data

All information handled in the business shall be classified (using four categories: open, internal, confidential and secret) and personal data processing operations shall undergo risk analysis to ensure an appropriate level of protection for both information and personal data. Appropriate protection shall be ensured throughout the entire lifecycle, i.e. during the definition of requirements prior to procurement, as well as during implementation, use/processing, development and finally the decommissioning of information systems/IT support. Appropriate safeguards shall also include risk-based background checks. The company shall have full insight into and control over the digital supply chain to ensure that all parties are compliant with the security and data protection requirements.

5.4. Internal reporting of various types of incidents relating to information security and data protection

Incident management forms part of the regular and systematic information security and data protection activities. Grant Thornton shall manage all incidents that occur, address any shortcomings and regularly follow up incidents to ensure a high level of protection for both business information and personal data. An important aspect of this work is being informed of any incidents that occur in daily operations, and this requires that all employees have the knowledge and skills needed to detect incidents. There shall be a process for internal reporting of security incidents and personal data incidents.

Public information. May be freely shared and distributed.

6. Compliance and monitoring

The policy owner has overall responsibility for the policy, which includes:

- Developing and regularly updating more detailed rules regarding the content of the policy, in accordance with the purpose and aim of this policy.
- Performing actions to communicate details about the policy and its underlying governing documents, to ensure good knowledge about them among employees.
- Monitoring the level of compliance with the policy.
- Where applicable, ensuring in the event of irregularities or serious deviations from the policy the taking of legal or disciplinary action, or assisting with this.
- Ensuring that any additional measures necessary to fulfil the purpose of the policy, including corrective actions and reporting, are taken.

Business Leaders are responsible for creating awareness of the policy and ensuring compliance with it in their respective Business Lines. The respective Head of Corporate Functions has the corresponding responsibility. Employees are expected to report material deviations from the policy to their line manager or to the policy owner.

7. References

The policy is supplemented by underlying instructions that contain more detailed rules regarding information security and data protection.

8. Version record

Version	Date	Comment
1.0	02.03.2026	First version of the policy in English.

Public information. May be freely shared and distributed.