Version: [1.1]

Valid from: [27.04.2023]

Grant Thornton Baltic's security requirements policy for suppliers

Purpose

Grant Thornton Baltic OÜ is committed to protecting Grant Thornton Baltic OÜ (hereinafter the company) users, partners, and the company from illegal or damaging actions by suppliers and third parties, either knowingly or unknowingly.

This SECURITY REQUIREMENTS POLICY FOR SUPPLIERS (hereinafter the policy) describes the security requirements that apply to suppliers and other third parties who do business with the company.

This policy applies to the services provided by the supplier considering the service includes at least one of the following activities:

- processes the company's data
- is allowed to stay unsupervised in the company's premises
- uses the company's network or IT systems, including remote access
- uses the company's information processing equipment
- provides of sensitive products and/or sensitive services and the company has identified the supplier as such.

Enforcement

The supplier agrees to apply and enforce this policy and the security measures and principles stated herein. The supplier legal representative confirms the policy by signing it.

If there is any failure to observe the policy, disciplinary measures may be taken. The measures which may be taken will vary according to the breach and its circumstances. However, the right is reserved to immediately revoke access and terminate the contract of any supplier who is in serious breach of this policy.

Revisions

This policy document will be reviewed and periodically revised annually or sooner where significant risk or change is identified in information systems and business practices. The company shall notify the supplier of any changes made to this policy 30 days in advance.

Principles of Supplier Security

The supplier is fully responsible for ensuring that the supplier's personnel comply with this policy.

The supplier must implement the measures necessary to comply with the policy before starting any task for the company.

At the company's request, the supplier informs the company about how the supplier complies with the policy and which measures have been taken by the supplier to comply with the policy.

The supplier informs the company at it@ee.gt.com of all security incidents (among others of personal data processing incidents) as soon as possible, but no later than 24 hours after detection of security incidents.

The supplier ensures that any processing of the company's data is in accordance with the policy.

The supplier does not allow any party access to the company's data without the company's prior written consent.

Managining Risks

The supplier must periodically identify, analyze, assess, and eliminate security risks.

Secure handling of information systems

The supplier uses systems, software and equipment that are safe for business. The supplier has defined and documented information security policy (or something similar) and procedures for security that must be confirmed by the supplier's management. They will be communicated to all appropriate supplier personnel.

Human Resources Related Security

The supplier shall ensure that all supplier personnel performing duties under the contract are reliable and compliant with any established security criteria.

Asset Management

Material assets

The supplier shall have an established and documented asset management system and shall maintain up-to-date records of all relevant assets and their owners. Assets include information, IT systems, backup copies of information and/or removable media, access rights, software, and configuration.

Data

The supplier implements measures to ensure accidental, unauthorized, or illegal loss of data in connection with the company transmitted, stored, or otherwise processed data.

The supplier returns or destroys (according to the company's decision) all the company's data and their copies of the contract at the end or at the company's request. The supplier confirms to the company in writing that the supplier has fulfilled this requirement.

Access Control

The supplier must have a defined and documented access control policy (including physical, logical, and remote access control).

Supplier must establish a process for giving user access and privilege access authorization and procedure for revocation of access rights.

Encryption

If encryption is required (Classification description and handling requirements) or according to the agreement between the parties, the supplier ensures encryption proper and effective use in accordance with industry's best practices.

Physical and Environmental Security

The supplier protects its data processing facilities from external and environmental threats and hazards. This includes securing the physical perimeter and access (door cards, keys etc.).

Operational Reliability

The supplier implements malware protection to ensure that the software used by the supplier to deliver products is protected from malware.

The supplier implements operational and technical security controls such as log management, firewalls, anti-virus, and encryption according to industry best practices.

Supplier shall back up critical information and test the backups to ensure recovery of information according to the agreement with the company.

Supplier's Subcontractors

The supplier must reflect the content of the policy in its contracts with subcontractors who perform tasks assigned under the contract.

At the company's request, the supplier shall provide the company with evidence that the subcontractor fulfils the supplier's security requirements.

Security Incident Management

The supplier must establish a security incident management procedure.

The supplier informs the company at it@ee.gt.com immediately after each security incident detection, but no later than 24 hours after the detection of incident.

All security incident reports shall be treated as confidential.

Business Continuity Management

The supplier must have documented processes and procedures for business continuity, including to comply with the disaster recovery plan.

The supplier contributes to the preparation of a mutual business continuity plan (BCP) and a disaster recovery plan (DRP) or updating at the company's request.

Compliance

The supplier shall comply with all relevant legal and contractual requirements, including those which are related to processing personal data (e.g., General Data Protection Regulation in EU).

At the company's request, the supplier shall provide the company with a report on compliance with security requirements.

At the company's request, the supplier informs the company about how the supplier fulfils the security requirements and what measures are taken to meet security requirements.

The supplier regularly monitors, reviews, and audits the subcontractor's compliance with security requirements.

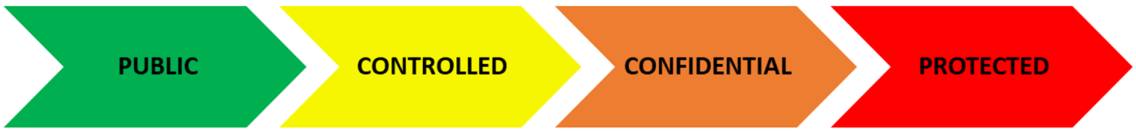
The company has the right to audit how the supplier and its subcontractors fulfil security requirements.

Classification Description and Handling Requirements

Information Classification

Four levels of classification apply to information at the company. It must be ensured that information is handled according to its protection level.

The sensitivity of an asset may change over time, and it may be necessary to reclassify assets.



Level	Potential Impact	Information Handling	Examples
Public	Disclosure is not limited to any person or group. The act of modification or disclosure would not result in any negative consequences for the organisation, the GT network, or our clients.	No restrictions Openly shareable internally and externally	Marketing material Service-related information Press releases Public company information (reg.code, location and official contact information, designated bank account), annual reports
Controlled (internal use)	Information that if modified or disclosed to inappropriate parties, could result in minor negative consequences to the organisation the GT network or our clients.	Employees and contractual clients/suppliers only With logical and physical access control Transmission using secure communication channels or a trusted network	Information provided for internal use Internal policies, guidelines, training materials and sessions Information regarding workflows and internal processes Information, documents and draft versions that are not treated as confidential
Confidential	Information that if modified or disclosed to unauthorised parties could result in material loss, moderate-high impact to operations or service delivery, serious contravention of regulations or other high risks to the organisation the GT network or our clients.	Known and acknowledged recipients or distribution lists only Logically and physically controlled and trusted storage with GT approved access control Transmission through secure communication channels, in a controlled and trusted network	Any Personally Identifiable Information (PII) Customer-identifying information Staff information Information bound to treat as confidential by the (potential) client (Client Agreements, Data Processing Agreements and NDA-s)
Protected	Information that if modified or disclosed to unauthorised parties could result in significant loss, severe impact on operations or service delivery, extensive and sustained negative publicity or other extreme risk to the organisation the GT network or our clients.	Specific employees/management only Logically and physically secure storage (encrypted or locked) Secure transmission (e.g., TLS 1.2)	Sensitive contracts Security information (e.g., passwords, details of security systems) Documents of high commercial or strategic value User health records

Contacts

For more information, please contact the IT team via e-mail it@ee.gt.com.

Grant Thornton

Learn more about our services, meet the team and read our insights:

grantthornton.ee

Grant Thornton Baltic - Estonia

grantthornton_estonia

GrantThorntonEstonia