Getinge Global Policy

IT Global Policy

Document owner	Agneta Palmér
Version	V3
Adopted by the Board of Directors	18 December 2023

1. Summary

Getinge Group is committed to protecting people and information, while at the same time mitigating overall IT risk. This Group Policy defines Getinge's standpoints in the area of IT, clarifying the behavior we expect from users, system administrators, management and IT security personnel. It also sets the safety standards for our IT system and applications. This Policy applies to all co-workers and business relations acting on behalf of Getinge Group.

2. Definitions

In this Global Policy, the following terms have the following meaning:

CIO	Chief Information Officer
CISO	Chief Information Security Officer
GDPR	General Data Protection Regulation (EU regulation on protecting personal data)
BYOD	Bring Your Own Device – a user's personal PC, tablet or mobile phone

3. Scope

This Global Policy is valid for all Getinge companies, its subsidiaries and joint operations (jointly "Getinge") and applies to all our employees and directors, as well as consultants and agency personnel who work at Getinge premises or under the direction of Getinge (all referred to in this Global Policy as "employees").

The objective of this Policy is to provide guidance and support for IT decisions within Getinge. It describes standards and procedures that reflect safe and acceptable practice based on accepted and current knowledge, guidelines and common practice.

4. Principles

Commitment and Expectations

The Getinge IT structure adds value by providing IT services to the company, balancing risk and reward with return on IT investment.

Getinge is committed to safeguarding people and information while mitigating overall IT risk. We direct and control our IT functions through structured management, a consistent process and by building strong relationships with the business.

The aim of this policy is to:

- Protect data and information;
- Set the rules for expected behavior by users, system administrators, management and IT security personnel;
- Set the standards for the IT system and applications;
- Mitigate overall IT risk.

We expect all employees and contractors accessing Getinge IT systems or hardware to follow this Policy and consistently apply its high standards.

5. Acceptable Use of IT Resources

Authorized Use: IT resources provided by Getinge are intended for business purposes in compliance with applicable laws, regulations, and industry standards. Personal use is acceptable as long as it does not interfere with job responsibilities or violate any other policies.

Prohibited Activities: The following activities are strictly prohibited:

- Unauthorized access to IT systems or data.
- Distribution, possession, or use of illegal or unauthorized software.
- Use of IT resources for any illegal or unethical activities.
- Unauthorized modification, destruction, or disclosure of data.
- Harassment, discrimination, or violation of the organization's code of conduct using IT resources.
- Any activity that compromises network or data security.

For further guidance please see: *IT Acceptable Use Directive*

6. Information Security

Cybersecurity

Defines how we manage cybersecurity and establish the security controls required to protect Getinge digital assets and data from threats:

- Adhere to established cybersecurity directive and procedures, which define rules and best practices for safeguarding data and technology resources.
- Regularly assess and identify cybersecurity risks that could impact the organization's information systems and data.
- Assess and manage the cybersecurity risks associated with third-party vendors and service providers.
- Regularly monitor systems for suspicious activities, conduct security audits, and comply with audit requirements.

All questions regarding cybersecurity shall be directed to Getinge's CISO.

For further guidance please see: *Cybersecurity Directive*

Data Management

- Employees must safeguard confidential and sensitive information. Data should be classified and handled according to Getinge's data classification directive.

For further guidance please see: *Data Management Directive*

Reporting Security Incidents

- All employees must promptly report any security incidents or suspected security breaches to the IT department or designated IT personnel.

For further guidance please see: *Cybersecurity Incident Directive*

Identity and Access Management Directive

- Ensures that access to sensitive systems and data is restricted to authorized personnel only, using strong authentication and authorization mechanisms.

For further guidance please see: *Identity and Access Management Directive*

Remote Access and Mobile Devices

- Remote access to Getinge network is permitted only through secure and authorized methods.

Training and Awareness

- Employees will receive training on IT security practices, and regular reminders will be sent to maintain awareness.

7. IT Equipment and Software

IT Operation

Establishes a baseline for IT operations to deliver stable and efficient IT services.

Covers areas like network security management, patch and vulnerability management, malicious code protection, logging and monitoring, and personal computer and mobile device management:

- Malware Protection: All devices connected to Getinge's network must have up-to-date antivirus and anti-malware software.
- Email Security: Only use IT approved email services that ensure that integrated systems comply with Getinge's security standards.
- Equipment Usage: IT equipment provided by Getinge is for business use. Any other equipment connected to the Getinge's network must comply with security standards.
- Software Installation: Installing software on Getinge's devices should be authorized by the IT department. Only use licensed software.
- Configure systems, devices, and applications securely to reduce the attack surface and minimize security risks.

For further guidance please see: *IT Operation Directive*

Data Backups

Ensure that there are plans in place to maintain essential operations.

- All critical data must be regularly backed up to prevent data loss. Employees are responsible for ensuring that important data is included in the IT backup process.

For further guidance please see*: IT Backup and Recovery Directive*

IT Governance

To ensure the efficient and secure delivery of IT projects and services, as well as to maintain global license compliance and uphold good purchasing practices for IT equipment and services:

- All IT projects must adhere to the Project Portfolio Management process and receive appropriate approvals.
- IT Licensing Management practices must be followed to maintain compliance with software license agreements.
- IT Procurement Management procedures should be followed for all IT-related procurement activities.

For further guidance please see: *IT Governance Directive*

IT Cloud Management

Outlines what to consider before selecting, implementing and operating cloud solutions or cloud services:

- IT must be involved in cloud purchasing processes (as early as possible).

For further guidance please see: *IT Cloud Directive*

Application Security

Ensures that security is integrated at the early stages of IT system development or acquisition.

For further guidance please see: *Application Security Directive*

8. Roles and Responsibilities

All Getinge employees are individually responsible for reading, understanding and complying with this Policy. Each employee is responsible for acting in accordance with this Policy,

Every line manager is responsible for making sure each team member has access to this Policy and related Directives, Instructions and Guidelines.

Day-to-day reinforcement, including regular information and training in the area of IT, as well as compliance follow-up, is part of every manager's responsibility, with the support of the IT Department

Violations against the Group Policy can lead to disciplinary action, up to and including termination.

9. Breaches against the Global Policy – Speak Up

Do not hesitate to raise a concern. Any Getinge employee who suspects violations of this Global Policy is expected to speak up and raise the issue to their line manager, to the Ethics and Compliance Office, or to use the Getinge Speak Up Line. The Getinge Speak Up Line is available on Getinge internal and external webpages. At Getinge we do not accept any form of retaliation against someone who speaks up, expressing concerns or opinions.

See further: Global Speak Up and Non-Retaliation Directive

10. Guidance and assistance

If there is a reason for not complying with any part of the IT Policy or IT Directives (e.g. legal, regulatory, financial or technical), an exception request must be filled out and sent to Getinge's Chief Information Security Officer and depending on the risk level additional approvals might be needed.

If you have questions on this Global Policy, please contact Pelle Nilsson, CIO.

Related Documents

- Cybersecurity Directive
- Cybersecurity Incident Directive
- IT Acceptable Use Directive
- IT Governance Directive
- IT Operation Directive
- IT Backup and Recovery Directive
- IT Cloud Directive
- Data Management Directive
- Identity and Access Management Directive
- Application Security Directive
- IT Security Exception Request