Getinge Policy

Global IT Policy

Document ID: POL-0128 rev1
Adopted by the Board of Directors 23-APR-2019

1. Summary

Getinge is committed to protect people and information, while at the same time mitigating overall IT risk. This 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.

2. Definitions

CFO - Chief Finance Officer

CIO - Chief Information Office

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

ITIL - Information Technology Infrastructure Library. A set of detailed practices for IT service management that focuses on aligning IT services with the needs of business.

3. Scope and Objective

This Policy is valid for all Getinge companies, its subsidiaries and joint operations (jointly "Getinge") and applies to all our employees, as well as consultants and agency personnel who work at Getinge premises or under the direction of Getinge (all referred to in this 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 the best possible service to the company, balancing risk and reward with return on IT investment.

Getinge is committed to safeguard people and information, while at the same time 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 people and information;
- Set the rules for expected behaviour 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. Further guidance is available in the underlying Directives and Instructions.

Information Security Directive

Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

The Getinge Information Security Directive defines how we manage Getinge Information Security risks, and establish the security controls required to protect Getinge information assets regardless of the form the data may take (e.g., electronic, or physical backups).

The aim of this Information Security Directive is to provide guidance on how, from a security point of view, we ensure:

- The confidentiality of our information.
- The access and availability of our systems.
- The integrity of our data.

The Information Security Directive applies to all computer information systems supporting Getinge business processes. This includes application infrastructure (including networks and communications), provided IT Services, desktop and laptop PCs, mobile devices (including phones, tablets, wearables), and personal devices, i.e. BYOD: s used for Getinge-related business.

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

For further guidance please see: *Information Security Directive DIR-0156*

Information Classification

The purpose of the Information Classification Directive is to ensure that Getinge information receives an appropriate level of protection based on the importance and sensitivity of this information and the systems that use it, thus reducing the risk of unauthorised disclosure, loss or damage to Getinge information.

All storage, use, transmission or deletion of data must adhere to the information classification. In case of a needed change to the use of data, this Directive identifies the restrictions, responsibilities and actions required. Any new data type must be classified. We always investigate new regulations that impact data security and/or privacy, and update accordingly.

For further guidance please see: *Information Security Directive DIR-0156*

IT Acceptable Use Directive

This Directive defines the acceptable use of Getinge IT resources to effectively manage and safeguard the use of all IT properties. This includes not only computers and mobiles, but also the use of electronic information systems (such as software, file shares), the Getinge network, Internet access and the electronic mail system.

These systems are used for business purposes, serving the interests of the company and of our clients and customers in the course of normal operations. All usage must be in accordance with applicable laws, ordinances, regulations and rules, and, where appropriate, with industry and consensus standards.

For further guidance please see: *IT Acceptable Use Directive DIR-0157*

IT Cloud Directive

Cloud computing is the delivery of computing services - servers, storage, databases, networking, software, analytics and more - over the internet ("the cloud").

This directive outlines what to consider before selecting, implementing and operating cloud solutions or cloud services:

- Clarifying key characteristics of cloud computing, service models and deployment models.
- Must-haves, best practices and forbidden things in the area of cloud.
- Recommendations and explanations why IT must be involved in cloud purchasing processes as early as possible.

For further guidance please see: *IT Cloud Directive DIR-0158*

5. Breaches against the Policy – Speak-up

Do not hesitate to raise a concern. Any Getinge employee who suspects violations of this Policy is expected to speak up and raise the issue to their line manager, to Human Resources to the Ethics and Compliance Office, or to use the Getinge Speak-Up Line. The 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, expresses concerns or opinions.

See further: Speak Up and Non Retaliation Instruction SOP-1305

6. 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 Policy can lead to disciplinary action, up to and including termination.

7. Exceptions to IT Policy and Directives

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.

IT Policy exceptions can only be approved by the Getinge Security Board, and depending on the risk level additional approvals might be needed.

All exception approvals must be limited in time and scope.

For further guidance please see https://intranet.getinge.com/en/our-company/it/it-security/security-exceptions/

8. Framework

This Policy is part of Getinge's Governance Framework, which includes:

- Code of Conduct, Our Cultural Core Values, Strategic framework, Policies approved by the Board of Directors, Directives approved by the CEO or direct reports to the CEO as well as local instructions
- Decisions made by the CEO or otherwise under the Delegations of Authority as approved by the CEO
- The Ethics and Compliance Office is responsible for ensuring that the latest version of this Policy is published and available to all employees on the Getinge intranet.
- This Policy will be reviewed every other year or as needed.
- The original language of this Policy is English.

9. Guidance and Assistance

To guide our conduct when it comes Getinge's standpoints in the area of IT there is this Policy and several directives, and instructions. If you have questions on this policy or you are uncertain which rules apply, please contact the Ethics & Compliance Office.

Useful Links:

Information Security Directive DIR-0156

IT Acceptable Use Directive DIR-0157

IT Cloud Directive DIR-0158

IT Security Exception Request Process