smit
Siseministeeriumi
infotehnoloogia-
ja arenduskeskus

DIRECTIVE

Tallinn 01.07.2025 No. 1-1/106

Information Security Procedure of the IT and Development Centre of the Ministry of the Interior

On the basis of § 10 section 2 of the Regulation No 8 of the Minister of the Interior of 17 February 2020 *Statutes of the IT and Development Centre of the Ministry of the Interior of Estonia:*

1. Hereby I enact the *Information Security Procedure of the IT and Development Centre of the Ministry of the Interior* appended to the directive.

2. The directive will enter into force on 1 August 2025.

3. As of 1 August 2025, I will repeal the directive of the Director General 1-1/25 *Information Security Procedure of the IT and Development Centre of the Ministry of the Interior* from 25 April 2024.

4. The head of the Information Security Department shall be in control of the execution of the directive.

ANNEXES:

Annex 1: Information Security Procedure of the IT and Development Centre of the Ministry of the Interior

(signed digitally)

Mart Nielsen
Director General

Annex 1. Information Security Procedure of the IT and Development Centre of the Ministry of the Interior

Table of contents

1. General provisions

1.1. The Information Security Procedure (hereinafter the Procedure) provides the principles and organisation of information security management, which is applied in ensuring the security of all the services and information assets of the IT and Development Centre of the Ministry of the Interior (hereinafter SMIT), including in guiding and regulating user behaviour, developing and managing information assets, planning and carrying out infrastructure changes, establishing procedures, guidelines and other rules.

1.2. The information security requirements established by the Procedure are based on the specifics of the internal security field, international and national regulations, best practice in the field and are in accordance with the ISO/IEC 27001 information security standard implemented in SMIT.

1.3. The purpose of the Procedure is to ensure the confidentiality, integrity and availability of services through the implementation of information security measures in accordance with the requirements and needs in all SMIT processes, thereby protecting the organisation as a whole and providing secure services to clients.

1.4. The Procedure does not regulate the processes related to state secrets and classified information of foreign states.

1.5. The Procedure applies to SMIT employees, trainees and external partners.

1.6. Violation of the requirements provided for in the Procedure is deemed to be a violation of the work obligation or contract. The Information Security Department may make the use of information systems subject to the completion of information security training and/or testing.

1.7. Information security manager organises compliance with the Procedure and the exceptions to the Procedure must be coordinated with the Information Security Department in a format which can be reproduced. The exception must be time-limited and justified.

1.8. The annual review and updating of the Procedure is organised by the head of the Information Security Department (hereinafter information security manager).

See also: The statutes of the Information Security Department

2. Definitions

2.1. **Data medium** is a medium for storing or transmission of data.

2.2. **Data network** is a SMIT user network and end-user devices.

2.3. **Information Security Management System (ISMS)** is a structured framework consisting of policies, procedures, guidelines, and related resources and activities that the organisation collectively manages in an effort to protect its assets.

2.4. **Information security** is a set of processes for creating, selecting and implementing security measures, as well as maintaining the confidentiality, integrity and availability of information.

2.5. **Information assets** are information, data and information technology applications necessary for their processing, as well as technical means or other assets that contain or carry valuable information for SMIT. For example, information, data, software, physical assets (infrastructure, building, hardware, equipment, etc.), financial assets, services, human resources (people, qualifications, skills, experience), know-how, non-material assets (reputation, image, etc.).

2.6. **Information asset user** is a person authorised to use the information asset.

2.7. **Information asset owner** is the person responsible for one or more information assets who allocates resources to ensure the security measures of those assets, confirms the controls, authorises access and monitors the performance of the controls.

2.8. **Removable media** is a device used to transport and store data or to provide mobile access to data. Removable media includes, for example, external hard drives, CDs, DVDs, magnetic tapes, memory cards, flash drives, SD cards, cameras, etc.

2.9. **Separation of duties** is allocating work process steps to people so that the approver of the action is not the person performing the action.

2.10. **Confidential information** is any non-public information intended for a limited number of persons and limited use.

2.11. **Confidentiality** is property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

2.12. **Availability** is the property of information, IT systems, people, processes to be accessible and usable on demand by an authorised entity.

2.13. **Vulnerability** is a vulnerable part of an information asset, control or process, a weakness (lack of security) that can be exploited in such a way that an event with a negative effect occurs. A weakness can be exploited by one or more threats.

2.14. **Threat** is an event or circumstance that has the potential to exploit a weakness and thereby cause the risk to materialise. The potential cause of an unwanted incident, which may result in harm to a system or organisation (an event or circumstance capable of taking advantage of the vulnerability).

2.15. **Client** for the purposes of this Procedure is an institution to whom SMIT provides information and communication technology (ICT) services. The client is represented by the **main user** of the respective service.

2.16. **Risk** is the effect of uncertainty on objectives. The effect is a deviation from the expected – positive or negative. Information security risks are usually associated with the negative impact of uncertainty on information security objectives. Risks are identified and evaluated in the course of risk assessment and kept under control through risk management.

2.17. **Integrity** is the accuracy and completeness of data, the absence of unauthorised changes, also includes authenticity and non-repudiation throughout the data life cycle.

2.18. **Product owner** is the owner of the ICT service and/or product specified in the SMIT Service Portfolio.

2.19. **Security incident** is an information security event that may damage the continuity and the information assets of SMIT and endanger the security of information.

2.20. **Data controller** is a legal person who determines the purposes and means of processing personal data, i.e. decides why and how personal data is processed. The data controller is responsible for ensuring that the data processing is carried out in accordance with the General Data Protection Regulation (GDPR) and legislation. In the SMIT's view, the data controller is mostly the client.

2.21. **Data processor** processes personal data on behalf of the data controller and only on the basis of documented instructions from the data controller, on the basis of a respective contract or legal act. The data processor shall not independently determine the purposes or means of personal data processing and is required to ensure security and compliance with the applicable data protection requirements upon processing of data. In the context of the area of government of the Ministry of the Interior data processor is SMIT.

2.22. **External partner** is an authorised representative of an organisation (contractual partner or supplier) operating under a contract providing services to SMIT, which performs contractual work for SMIT and requires access to the information assets managed by SMIT (including information systems, data or physical infrastructure), in accordance with agreed terms and access rights.

3. Roles and responsibilities

3.1. The principle of separation of duties is applied in ensuring information security, monitoring and service management, ensuring that different tasks and powers are allocated in such a way as to reduce potential risks and conflicts and to ensure security and transparency.

3.2. The implementation of the Information Security Procedure and the operation of the ISMS is the responsibility of the Director General of SMIT, supported and advised by the heads of structural units (Deputy Director General in Business Services, Deputy Director General in Basic Services, Deputy Director General in Human and Culture, Head of Strategy, Head of Law and Procurement and Head of Finance).

3.3. The Director General, in cooperation with the heads of the structural units, ensures that the ISMS complies with the strategic objectives of SMIT, is integrated into business processes, policy design and formulation as well as availability of resources.

3.4. The Deputy Directors General are responsible for the functioning of the ISMS in their area.

3.5. The information security manager is responsible for ensuring compliance of the ISMS with the Information Security Standard applied in SMIT and informs the Director General of the information security activities and results. The information security manager at SMIT is the head of the Information Security Department whose rights, obligations and responsibilities are set out in the Information Security Policy of the Area of Government of the Ministry of the Interior, the Statutes of the Information Security Department, his or her employment contract and other documents.

3.6. The risk manager is responsible for the implementation of SMIT Risk Management Policy, the organisation of the risk assessment and annual review of risks, and the overall coordination of the implementation of ISMS, document management and monitoring of the implementation of improvements to the ISMS.

3.7. The internal auditor reviews the functioning of the ISMS once a year, involving internal and external experts, if necessary.

3.8. The overall responsibility for information security lies with each employee. The employee must comply with the information security requirements, the orders of the information security manager and must notify the Information Security Department of any discovered security incidents, vulnerabilities, potential security events or other security threats to SMIT or the services provided or suspicions thereof.

3.9. Within the limits of their services, the responsibility for information security of the services lies with the head of a structural unit or department, who organises, is responsible for and supervises the implementation of the requirements arising from the Procedure and the specifics of the service and the data handled therein in his or her area of responsibility. The head of the structural unit or department has the right to make decisions regarding their services and their interfaces in order to ensure the security of services and the data processed there in accordance with information security requirements. Specific information security requirements for services and processes are described in the WIKI Information Security Guidelines and the Main Process.

3.10. The head of the structural unit or department supervises the access to and use of data processed in the services, including of data used for testing of the services and the creation of additional environments. As the data processor, he or she coordinates changes and requirements in data and service environments/information assets, including data, with the data controller (on the terms and conditions set out in Service Desk or in the contract).

3.11. The head of the structural unit or department may delegate the rights, obligations and responsibilities described in clauses 3.9 and 3.10, for example, to product owners, architects, etc.

3.12. The product owner is responsible for the implementation of the requirements applicable to the service arising from legal acts and contracts. Service and supply contracts must also include the obligation and procedure to notify of security vulnerabilities, data leaks, attacks and other threats and incidents affecting the service or product.

3.13. The client or a person authorised by the client has the right to verify the compliance with the agreed requirements and the business continuity of the service (e.g. whether the service continuity plan has been prepared, tested, existence and preservation of logs, etc.), including compliance with requirements and responsibilities (e.g. central log management, development requirements, compliance with business continuity requirements, compliance with Information Security Procedure, etc.).

3.14. It is the responsibility of the product owner to ensure the continuity of the service according to the agreed levels of availability, confidentiality and integrity, and to arrange for the timely elimination of malfunctions and security vulnerabilities. The acceptance and mitigation of risks in other ways should be justified and proportionate and should comply with the requirements of the Risk Management Policy.

3.15. Central information security responsibilities and general cross-service security requirements are developed by the Information Security Department.

See also: Statutes of the Information Security Department, ISO 27001 Information Security Management Manual, Requirements for Organisation of Business Continuity, Main Process, Risk Management Policy, Information Security Policy of the Area of Government of the Ministry of the Interior

4. **Security of staff**

4.1. All job candidates, candidates for traineeships and external partners providing services to SMIT will be subject to a background check. Background checks follow the rules arising from legislation. Anyone who is expected to pass a background check will be notified of the background check. The background check will be carried out on the basis of the completion of the consent form. Background checks are carried out by the Police and Border Guard Board on the basis of the Police and Border Guard Act.

4.2. The application of the information security rules in the recruitment of staff is organised by the HR Department and coordinated with the information security manager.

4.3. The prerequisite for concluding the employment contract is successful passing the background check and getting acquainted with the Procedure. It is prohibited to enter into a contract or allow the performance of an external partner's contract before the outcome of the background check is known.

4.4. In order to improve and deepen information security knowledge, security training and exercises are organised as necessary, and information security coaching for staff will be provided. Every employee is required to complete information security training at least once a year, and a new employee is required to complete it during the probationary period.

4.5. Operational security communication of personnel is carried out via e-mail, intranet, mobile phone and/or messaging service.

See also: Background Checks of External Partners and Requests for Access Rights

5. **Handling of data media**

5.1. The data media must be marked and stored in such a way as to ensure, where appropriate, that they can be located and used by a replacement employee or other authorised person.

5.2. Confidential data on digital media must be marked, encrypted and stored in locked cabinet in workspaces.

5.3. Data media used by SMIT, which have become unnecessary and which are not subject to storage, must be destroyed in accordance with the applicable procedures.

5.4. In the event of destruction or re-use of data media, the user and/or the owner together with the data controller assesses the necessity of storing or destroying the data on the data medium.

5.5. The back-up and recovery of data is governed by the applicable procedure "Requirements for the Organisation of Business Continuity" approved by the Director General.

5.6. Any loss or theft of any data medium or device issued by SMIT or the possibility of third party access to its data must be immediately notified to Customer Support.

5.7. Only removable media issued by SMIT may be used for the processing, including storage and transport, of work-related data.

5.8. The removable media used in SMIT must support hardware encryption, be entered and registered in accordance with the requirements of the Asset Management and Accounting Procedures and registered under the responsibility of the user.

5.9. Removable media necessary for the performance of the duties which are not issued by SMIT must not be connected to a centrally managed device issued by SMIT. To receive data from such removable media, one must use a removable media kiosk or give the device to a SMIT IT technician who will retrieve the data from it.

5.10. Removable media and external data media issued by SMIT that have been connected to a device outside the area of government must be checked at an removable media kiosk or given to a SMIT IT technician for inspection before connecting to a SMIT computer.

5.11. The removable medium may only be used with the consent of the data controller for the recovery of data in a crisis situation or transport, but may not be used for permanent storage of ICT service/database data. As data processor, SMIT stores the services/database data in data centers and backups the data in accordance with the requirements agreed with the data controller and the applicable procedures. The respective operations and agreements between the data controller and the data processor are documented in the Service Portfolio.

See also: Asset Management and Accounting Procedures, Document Classification Scheme, Requirements for Organisation of Business Continuity, Service Portfolio

6. **Regulation of access to information**

6.1. An employee and an external partner may have access only to the information, database, network and network services that they need to use for their duties.

6.2. Each staff member and, where appropriate, an external partner will be provided with technical tools supporting two-factor authentication and will be granted access rights to information assets, as required for the performance of their duties, under the Procedures for the Management of Electronic Access, provided that:

6.2.1. he/she is familiar with this Procedure and undertakes to comply with it;

6.2.2. he/she has the necessary access permit for processing the relevant data due to his/her duties (e.g. granting of the right of access is coordinated with the data controller) and a justified need to know.

6.3. Every employee and, if necessary, an external partner must have two-factor authentication capability accepted by SMIT.

6.4. The Information Security Department coordinates and technically supervises the granting of privileged access rights.

See also: Procedure for Management of Electronic Access

7. Security of the physical environment

7.1. Physical environment security includes the management of the processes ensuring the physical security of SMIT assets and all information assets owned by SMIT or provided to SMIT for hosting.

7.2. Physical environment security, including the implementation of the applicable security requirements, is organised by the head of Administration Department, who coordinates them with the SMIT information security manager.

7.3. Access to SMIT's assets is only permitted for the performance of duties.

7.4. In addition to the security requirements agreed in writing with SMIT, SMIT workplaces and SMIT assets held at contractual partners or clients are subject to the physical security measures of partners or clients.

7.5. When placing and using ICT tools, care should be taken to ensure that they cannot be used and moved without authorisation, including by viewing the information contained therein and using the data therein without authorisation.

7.6. The user must exclude unauthorised persons from access to the information assets.

7.7. Outside the locations of the institutions within the area of government of the Ministry of the Interior, employees are not permitted to leave the ICT tools granted to them without supervision in unlocked rooms or public places that could facilitate their theft, destruction or other exploitation.

7.8. The controls resulting from the physical security requirements are implemented in accordance with the security needs of buildings and premises, taking into account the value of the assets to be protected.

See also: Procedure for Using Computer Workplace, Procedure for Using Mobile Devices and Services and Covering Costs, Procedure for Using Server and Device Rooms, Procedure for Accessing SMIT Premises, SMIT Rules of Work Organisation, Procedure for Using SMIT Work Devices Abroad

8. Infrastructure management and network security

8.1. The used hardware and software covered by the commercial license must have the support of the manufacturer, with the exception of specific software in situations of unavoidable need and weighted risk. This is assessed by the Information Security Department on the basis of the explanations given by the product owner. In a situation where it is not possible to replace the legacy software, the head of the respective structural unit is responsible for the security of the legacy software and the related risks.

8.2. The technical documentation of the hardware and software used in SMIT must be protected against unauthorised access, exceptions must be coordinated with the Information Security Department.

8.3. The SMIT data network shall be structured in such a way that different user segments are logically separated from each other.

8.4. For data communication between segments, the minimum number of connections must be used, and data communication between segments must pass through a firewall and be encrypted, if possible.

8.5. All devices connected to the SMIT data network must be identifiable and have a corresponding network certificate (IEEE 802.1x).

8.6. Access to internal network resources through a public network and transmission of confidential data over an external network is only allowed via a secure virtual private network (VPN). The VPN software must be configured in such a way that at least two-factor authentication is required to connect. Exceptions must be coordinated with the Information Security Department.

See also: Software Management Procedure, Network Management Procedure

9. **Standard configuration of workstations**

9.1. As a rule, SMIT computer workplaces have a standard configuration and are managed centrally. SMIT employees are not allowed to change the security settings or configuration of the devices they use, including interrupting the processes that are automatically started on the device (e.g. anti-malware, end device protection solution, etc.).

9.2. The configuration of the software, the software used and its updating for computer workplaces with a standard configuration are decided by and under the responsibility of the Workplace Services Department.

9.3. Decisions to improve the software profile are taken by the Workplace Services Department, assessing the need for the software to be added, licensing terms, central administration, security patching possibilities, availability of alternatives in the software profile, etc. The prerequisite for the implementation of the new software is the coordination of the Information Security Department.

9.4. The use of a computer workstation configuration other than the standard configuration is permitted as an exception if the need arises from work duties and is coordinated with the Information Security Department.

9.5. When using a computer other than the standard configuration, the user of the computer is responsible for the implementation of controls intended to ensure information security, which are also applied to standard computer workstations, and for ensuring the requirements of the Procedure. The user of the device is fully responsible for the processing of the data in the device, the security of the device and the data, as well as the operation, configuration and security patching of the device.

See also: Procedure for Using Computer Workplace, Software Management Procedure

10. **Information asset security**

10.1. Only authorised software may be installed on SMIT computers for the performance of the duties. The list of authorised software and the instructions for coordinating the requested software are described in the Software Catalogue.

10.2. Employees are not allowed to store and print work-related information in IT systems and devices that are not managed by SMIT, unless this is required by law.

10.3. Employees are not allowed to misuse the features of information systems or additional resources (software or hardware) to obtain privileged access rights or disrupt the operation of IT systems.

10.4. Upon notification, the user must restart the device to load system updates. If this is ignored, the device may restart itself. It is permitted to postpone the restart for a reasonable period in order to complete the work that is currently in progress at the time of the notification.

10.5. When a malware warning appears on the screen, the user must immediately notify SMIT Customer Support and wait for further instructions from the Customer Support/Information Security Department to perform the necessary operations. Before that, any action, including independently removing malware, is prohibited.

10.6. The SMIT employee may not redistribute the SMIT network to non-SMIT users without authorisation, using, for example, Bluetooth, 4G, WiFi, etc.

10.7. The use of Bluetooth accessories on SMIT computers and phones is prohibited for processing information intended for internal use, except for computer mice. The use of headphones and microphones for the processing of information for internal use is only allowed via a cable connection and the Bluetooth connection must be switched off on such devices. Bluetooth headphones are allowed if they do not process information for internal use (for example, listening to podcasts or music).

10.8. It is not allowed to connect personal devices to the computer network of the area of government of the Ministry of the Interior (except for the SMIT public WiFi network) without the SMIT VPN solution.

10.9. It is prohibited to connect SMIT devices to public charging points (e.g. in airports, etc.) using a USB cable. The user may only connect the following personal devices to the SMIT device: monitor, keyboard, mouse, docking station, secured router, SMIT's centrally managed mobile device.

10.10. The rules for going abroad with a SMIT device (for any reason) and for working remotely from abroad are agreed upon by the employee and the manager specified in his or her employment contract, following this Procedure and cooperation agreements described in the Procedure for Using SMIT Work Devices Abroad.

See also: Procedure for Using Computer Workplace, Software Management Procedure, Procedure for Using Mobile Devices and Services and Covering Costs, Procedure for Using SMIT Work Devices Abroad

11. **E-mail and instant messaging**

11.1. All e-mail traffic from the SMIT network or to the SMIT network must pass through the e-mail server managed by SMIT. Only an e-mail address managed by SMIT may be used for electronic correspondence related to work duties.

11.2. Correspondence not related to work duties (for example, payslips, communication between employees and teams to agree on an external meeting) must be clearly distinguished, for example, by a folder titled "Personal".

11.3. The employee is obliged to check the correctness of the addressees when sending an e-mail.

11.4. The employee is obliged to make sure that the message sent does not contain unnecessary information for the addressees and to ensure that information subject to access restrictions does not fall into the hands of unauthorised persons.

11.5. Information sent electronically outside the area of government of the Ministry of the Interior and classified for internal use must be encrypted by the employee or otherwise protected from unauthorised processing.

11.6. The employee must make sure that the links and files received by e-mail are safe before opening them regardless of the sender's identity. In case of doubt, the e-mail must be sent to spam@smit.ee. Files can be checked with the file security check system or by sending files and/or links to file sharing environments to failikontroll@smit.ee. Verified files can be downloaded from the appropriate environment. If you click on a link, attachment, etc. that contains malware, you must immediately notify Customer Support.

11.7. E-mails sent to the external network by the employee must include the sender's real name.

11.8. Owner of the department's or structural unit's mailing list is the head of the relevant unit or an employee delegated by the head of the unit. The owner of the mailing list has the obligation to keep the e-mail recipients of the mailing list up to date and to submit a request to Customer Support to delete the mailing list if there is no further need for the mailing list. The owner of the mailing list is allowed to assign only the e-mail addresses of the area of government of the Ministry of the Interior to the mailing lists.

11.9. Personal e-mail or personal instant communication applications may not be used to exchange information for internal use. All work-related communication must be carried out only through official and secure channels of SMIT.

11.10. For file and instant messaging, work-related information may be transmitted using applications authorised by SMIT that can be found in the software catalogue.

See also: Rules of Work Organisation, Software Management Procedure

12. **Acquisition, development and maintenance of systems**

12.1. The owner of the information asset must apply the necessary security measures to the information asset in accordance with the requirements established by the Information Security Department and the applicable procedures and legal provisions.

12.2. Structural units must identify their information assets, document them properly, assign their security level (security class) and owner. The product owner must document their services in the Service Portfolio and keep them up to date. The information assets, environments, business continuity requirements, dependent services and the impact on other services necessary for the provision of the service must be described, among other things.

12.3. The security level of the data processed in the service is determined by the main user representing the client, who must in advance assess the importance of the data and the losses caused by the lack of data security.

12.4. In the case of data in a database, the security level and security class must be determined by the data controller of the database.

12.5. The security level and security class are determined on the basis of § 7–10 of the Regulation "Cybersecurity requirements for Network and Information Systems" of Government of the Estonian Republic of 13 December 2022 (https://www.riigiteataja.ee/akt/113122022030).

12.6. The planning of SMIT services must follow development requirements (ICT Development Process) and good practices of development and security.

12.7. Changes to the services must be thoroughly analysed by the product owner from an information security point of view, the risks associated with the change must be assessed, and the product owner must coordinate with the client and Information Security Department before implementing the changes. In the event of changed requirements and/or emerging threats, any changes in the subclasses of availability, confidentiality and integrity must be reviewed and, if necessary, security measures amended. The changes must be described in the Service Portfolio.

12.8. If a security vulnerability is detected in a service-related application, the product owner or other person responsible for the application must notify the Information Security Department and the client and correct the vulnerability in accordance with the requirements. The Information Security Department monitors and coordinates the elimination of security vulnerabilities and, if necessary, provides information about the identified security vulnerability to the ICT service owner.

12.9. The data processed in the performance of SMIT's tasks must be fit for purpose, reliable and complete, in accordance with the requirements of the client/data controller. Copying data without the need and increasing the number of copies should be avoided. In cases where the making of a copy is unavoidable, this must be done in accordance with SMIT's Procedure for Generating and Administration of Extraordinary Copies.

12.10. The processes for acquiring, using, managing and exiting cloud services must comply with the requirements established by the Information Security Department and the applicable procedures and legal regulations. The requirements for the security measures of the network and information system and the extent of their application in the use of cloud services are regulated by Regulation No. 1 of the Government of the Estonian Republic from 3 January 2024 (https://www.riigiteataja.ee/akt/109012024025). Information sent via cloud services classified for internal use must be encrypted by the employee or otherwise protected from unauthorised processing.

12.11. Users of the service and information assets and the operations performed by them must be unambiguously identifiable and logged.

12.12. Development, testing and operating environments must be separate from each other.

See also: ICT Development Process, General Conditions of ICT Services, Change Management Procedure, Requirements for Organisation of Business Continuity, Main Process, SMIT's Procedure for Generating and Administration of Extraordinary Copies, Procedure for Security Testing, Vulnerability Management and Logging Requirements for Information Systems within the Area of Government of the Ministry of the Interior, Service Portfolio

13. **External partners**

13.1. A background check will be carried out for all external partners.

13.2. The head of the structural unit or department in whose area of responsibility the activities of an external partner are carried out, organises the activities of the external partner and ensures their compliance with the procedures.

13.3. The procedures and requirements applicable to the external partner will be included in the tender specifications.

13.4. To connect to SMIT environments, an external partner uses either a SMIT workstation or a personal device. The use of the SMIT workstation is mandatory for administrative operations, which also includes issuing the necessary administrative accesses (privileged user account), exceptions must be coordinated with the Information Security Department.

13.5. When going abroad with a SMIT workstation and working remotely from abroad, the external partner must follow the Procedure for Using SMIT Work Devices Abroad.

13.6. The external partner must be aware of the consequences of a wrongful breach of security requirements. In case of violation of security requirements and principles, sanctions may be imposed on the external partner, including claiming compensation for the damage caused by the external partner pursuant to the provisions of the contract.

13.7. The external partner is obliged to inform the head of the structural unit or department responsible for the activities of the external partner, of any security vulnerability detected, potential security event or other security threat.

See also: Guidance on Applying for Background Checks and Access Rights of External Partners, Procedure for Using SMIT Work Devices Abroad

14. **Management of security incidents**

14.1. Data on the use of the information system related to the user are collected for the purpose of identifying prohibited activities (e.g. events, incidents) provided for in this Procedure and other legislation regulating information security.

14.2. The collection of data on the use of the information system and the network is automated and the processing of data can be both automatic and manual.

14.3. The SMIT Information Security Department shall have the right to decrypt, inspect, monitor and store all data traffic or direct it through appropriate control mechanisms to ensure that information is protected in accordance with the purpose set out in clause 14.1 of the Procedure.

14.4. The SMIT Information Security Department and Customer Support have the right to identify the physical location of the devices given to the user, including by using the GPS interface of the device, in order to resolve the incident.

14.5. The SMIT Information Security Department is obliged to register the identified security events and/or incidents, coordinate their resolution and assist the product/service team, Customer Support Department and/or clients in resolving them. For security reasons, the SMIT Information Security Department has the right to restrict access to security events and incidents.

14.6. The user must immediately notify SMIT Customer Support and/or Information Security Department of a security incident.

14.7. The user is obliged to contribute in every way to the investigation and resolution of the incident by ensuring necessary access to the equipment issued by the area of government of the Ministry of the Interior and providing oral or written explanations at the request of the structural unit or department investigating the incident.

14.8. The SMIT Information Security Department shall have the right to partially or completely suspend the network traffic or use of individual workstations or applications by informing the user of a prohibited activity or a security incident and instructing the user to prevent security incidents in the future. The SMIT Information Security Department also has the right to completely delete the content of the ICT devices provided to the user in order to prevent the escalation of a security incident.

See also: Instructions for Handling Security Incidents

15. **Requirement of confidentiality**

15.1. The requirement of confidentiality applies to confidential information and is independent of the official position or physical employment of persons and also applies to employees who do not have direct authority to use information assets.

15.2. For SMIT, confidential information means information, the disclosure or unauthorised receipt of which could harm the functioning, security or other essential interests of SMIT, such as, but not limited to:

15.2.1. internal documents and reports that are not public;
15.2.2. contracts that contain trade secrets or sensitive information and are not public;
15.2.3. data on SMIT information systems and technical solutions that may be targeted at cyber attacks;
15.2.4. personal data and other data the disclosure of which violates privacy or law;
15.2.5. state secrets;
15.2.6. physical security measures;
15.2.7. privileged rights and their users;
15.2.8. national defense jobs.

15.3. An employee who accidentally comes into contact with confidential data in the performance of his or her duties or in the course of his or her work undertakes:

15.3.1. not to disclose or transfer to third parties any confidential information which has become known to him or her, except in cases provided for by law;
15.3.2. to comply with applicable data protection legislation and procedures;
15.3.3. to comply with the confidentiality obligation both during and after the employment relationship has ended to the extent provided by legislation.

15.4. If a person performs works on the basis of a contract under the law of obligations, the confidentiality provisions of the contract must contain the principles set out in clause 15.3 of the Procedure.

See also: Rules of Work Organisation