Approved by order No 209 of 04.12.2024 of the Director for Administration

In force from: 04.12.2024

Rules for the Management and Use of End-User Devices

1. General provisions

1.1 The Rules for the Management and Use of End-User Devices (hereinafter referred to as “the Rules”) have been established to ensure the security of information technology assets and data of Tallinn University of Technology (hereinafter referred to as “the university”), in compliance with the ISO/IEC 27001 standard. The Rules apply to all university employees, students and partners using the devices and services managed by the university. The Rules govern the use of end-user devices that are centrally managed and those that are not centrally managed to ensure the security and protection of information across the university's networks and systems.

1.2 For the purposes of the Rules, “**a device**” means any electronic device with computing capabilities used to perform the functions of Tallinn University of Technology or to access its systems and networks. Devices include personal and portable computers, servers, mobile workstations (such as smartphones), and other similar devices intended for performing computing, data processing, communication, or management tasks.

1.3 For the purposes of the Rules, “**centralised management**” means centralised operations of the Information Technology Services to ensure unified management, security and reliability of the university’s devices and systems. This encompasses installing and updating operating systems, software, and security patches, managing device configurations and profiles, remotely monitoring devices to prevent security issues, implementing data protection measures such as device encryption and antivirus software, and administering user access rights. The aim of centralised management is to ensure that all managed devices comply with the university’s information security and technical requirements while facilitating seamless work processes.

2. Scope of application

2.1 The Rules apply to all university employees and students and cover the following activities:
2.1.1 use of centrally managed devices;
2.1.2 use of devices not managed centrally;
2.1.3 management of end-user devices;
2.1.4 commissioning, use, decommissioning, and destruction of devices;
2.1.5 ensuring security, data protection and privacy.

3. User device profiles

3.1 Computers in computer labs and auditoriums

3.1.1 Profile description:
3.1.1.1 the devices are fully managed by the university’s Information Technology Services. All software updates and security patches are installed centrally. Drivers are regularly updated to ensure the reliability of connected devices;
3.1.1.2 the Information Technology Services shall ensure information security, including the installation of antivirus software that is updated automatically;
3.1.1.3 device login is performed using a UNI-ID account. Users (including students) do not have administrator rights;
3.1.1.4 user profiles, along with associated files and data, are regularly deleted from devices.
3.1.2 Users’ roles and responsibilities:
3.1.2.1 users have access to pre-installed software;
3.1.2.2 users are responsible for following the instructions for using the university’s computer labs;
3.1.2.3 users are required to promptly notify the IT Helpdesk of any issues or anomalies encountered while using a device.
3.1.3 Management process:
3.1.3.1 software updates and security patches are installed automatically;
3.1.3.2 the operation and security of the system are continuously monitored by using management software;

3.1.3.3 user profiles are automatically deleted from devices.

3.2 End-user devices

3.2.1 The following general rules apply to end-user devices used to carry out the organisation's functions:

3.2.1.1 users are entitled to receive support and guidance from the Information Technology Services on the use of devices, installation of software, and resolution of technical issues;

3.2.1.2 users are entitled to use the devices to perform work tasks in accordance with the device profile and the university's guidelines and policies;

3.2.1.3 users are responsible for securing the data on their devices and must adhere to the university's information security guidelines and policies to ensure its protection;

3.2.1.4 if a user is using a fully managed device, data backups are performed in accordance with the organisation's IT management policies and systems;

3.2.1.5 if a user is using a partially managed or personal device, the user is responsible for backing up the data on the device;

3.2.1.6 disabling antivirus solutions and logging processes is prohibited;

3.2.1.7 the use of unlicensed software on university devices and systems is prohibited;

3.2.1.8 device use, including software updates, antivirus protection, and encryption must comply with the security requirements and guidelines established by the university.

3.3 Fully centrally managed Windows devices

3.3.1 Profile description:

3.3.1.1 the devices are fully managed by the university's Information Technology Services. All software updates and security patches are installed centrally. Drivers are regularly updated to ensure the reliability of connected devices;

3.3.1.2 device login is performed using a UNI-ID account. Users do not have administrator rights;

3.3.1.3 the storage drives of the devices are encrypted with BitLocker. Cryptographic keys are stored in the management software linked to the device record;

3.3.1.4 the Information Technology Services installs the default software on the device that corresponds to the profile. The university provides additional software to users, which is included in the central software repository. Users can install additional software on their devices using the university's central software repository. All centrally installed software is licensed. If additional software is required, its installation must be requested from the IT Helpdesk;

3.3.1.5 in the event of device failure, a replacement can be provided to ensure uninterrupted work;

3.3.1.6 after installation, there will be a centrally managed administrator account created on the device for IT Helpdesk.

3.3.2 Users' responsibilities:

3.3.2.1 the user shall use the device primarily to perform work-related tasks. Personal use (e.g., sending emails, browsing the web) is allowed within reasonable limits, as long as it does not compromise the device's reliability or violate the university's information security requirements;

3.3.2.2 changing a device's hostname is prohibited;

3.3.2.3 users cannot install or remove software;

3.3.2.4 users are required to promptly notify the Information Technology Services of any problems or anomalies;

3.3.2.4.1 users must adhere to the university's information security guidelines and policies.

3.3.2.5 Management process:

3.3.2.5.1 the Information Technology Services continuously monitors the system's proper operation and security;

3.3.2.5.2 software is installed and updated automatically;

3.3.2.5.3 if security vulnerabilities are identified, remediation measures are implemented in accordance with the Security Vulnerability Management Procedure.

3.4 Centrally managed Windows devices of users with privileged access rights

3.4.1 Profile description:

3.4.1.1 the devices are fully managed by the university's Information Technology Services, but users have been granted privileged access rights to manage their devices (local administrator rights). Users can install and uninstall software. All software updates and security patches are installed centrally (excluding software installed by the user). Drivers are regularly updated to ensure the reliability of connected devices;

3.4.1.2 device login is performed using a UNI-ID account;

3.4.1.3 the storage drives of the devices are encrypted with BitLocker. Cryptographic keys are stored in the management software linked to the device record;
3.4.1.4 the Information Technology Services installs the default software on the device that corresponds to the profile. The university provides additional software to users, which is included in the central software repository. Users can install additional software on their devices using the central software repository;
3.4.1.5 the Information Technology Services provides user support for the device. In the event of major, time-consuming issues, the device will be reinstalled, and all existing data and software will be deleted;
3.4.1.6 in the event of device failure, a replacement can be provided to ensure uninterrupted work;
3.4.1.7 after installation, the device will have two local user accounts:
3.4.1.7.1 the admin account (with administrator rights): intended for the end user to perform tasks that require special privileges. The user enters the appropriate password upon receiving the device;
3.4.1.7.2 the central management admin account: intended for the use by the IT Helpdesk of the Information Technology Services. This account must not be deactivated, as doing so would prevent the IT Helpdesk from accessing and managing the device.
3.4.1.8 Users' responsibilities:
3.4.1.8.1 the user shall use the device primarily to perform work-related tasks. Personal use (e.g., sending emails, browsing the web) is allowed within reasonable limits, as long as it does not compromise the device's reliability or violate the university's information security requirements;
3.4.1.8.2 users are responsible for ensuring the proper operation of the software and systems they have installed;
3.4.1.8.3 changing a device's hostname is prohibited;
3.4.1.8.4 users must regularly install security patches and updates;
3.4.1.8.5 the user shall use the standard user account to perform work tasks. The use of an admin account is permitted only for performing work-related activities that require special privileges;
3.4.1.8.6 users bear full responsibility for all actions performed using the admin account. The user is responsible for technical issues that he/she might encounter with the device and the IT Helpdesk will only provide support by performing a recovery installation;
3.4.1.8.7 disabling antivirus software and logging processes is prohibited.
3.4.1.9 Management process:
3.4.1.9.1 the Information Technology Services continuously monitors the system's proper operation and security;
3.4.1.9.2 software is installed and updated automatically;
3.4.1.9.3 the Information Technology Services conduct regular audits to ensure adherence to security requirements.
3.4.2 Devices not managed by the Information Technology Services.
3.4.2.1 Profile description:
3.4.2.1.1 devices purchased by the university that are not managed by the university's Information Technology Services. Users can install and uninstall software. The end user is responsible for installing software updates, security patches, and drivers;
3.4.2.1.2 the Information Technology Services provides assistance in ensuring information security, including installing automatically updated antivirus software on Windows and macOS devices.
3.4.2.1.3 as a rule, device login is performed using a local account;
3.4.2.1.4 data on the devices is not encrypted by default. The user is responsible for encrypting data and storing keys;
3.4.2.1.5 The files on the device are not backed up. The user is responsible for selecting and configuring the backup solution. The Information Technology Services recommends using the Microsoft OneDrive solution;
3.4.2.1.6 the Information Technology Services provides user support for these devices on a best-effort basis.
3.4.2.2 Users' roles and responsibilities:
3.4.2.2.1 the user shall use the device primarily to perform work-related tasks. Personal use (e.g., sending emails, browsing the web) is allowed within reasonable limits, as long as it does not compromise the device's reliability or violate the university's information security requirements;
3.4.2.2.2 users are responsible for ensuring the proper operation of the software and systems they have installed;
3.4.2.2.3 users are required to use only official and licensed software;

3.4.2.2.4 users shall install all essential security patches and updates;
3.4.2.2.5 users shall use strong passwords and adhere to best practices in information security;
3.4.2.2.6 administrator rights may only be used to make configuration or software changes required for work tasks. Standard user rights should be used for daily tasks to minimize information security risks;
3.4.2.2.7 the user is responsible for backing up the data on the device;
3.4.2.2.8 disabling antivirus software and logging processes is prohibited;
3.4.2.2.9 users bear full responsibility for all actions performed using the device. The user is responsible for technical issues that he/she might encounter with the device and the IT Helpdesk will only provide assistance by performing a recovery installation.
3.4.2.3 Management process:
3.4.2.3.1 the Information Technology Services monitors the proper operation and security of the system and provides guidance and advice to ensure security;
3.4.2.3.2 network traffic and device connections are secured through network segmentation and the implementation of security policies.

3.5 End-user computers, phones, and tablets that are not purchased or managed by the university (hereinafter referred to as "BYOD devices").

3.5.1 Profile description:
3.5.1.1 users' personal computers, tablets, and mobile devices connected to the university network or accessing services with the university UNI-ID account.
3.5.2 Users' roles and responsibilities:
3.5.2.1 The use of personal devices to access university networks and systems is allowed; however, the following information security requirements must be met:
3.5.2.1.1 BYOD devices must comply with minimum security requirements, including, but not limited to the following:
3.5.2.1.2 the device must have an up-to-date operating system and the latest security updates installed;
3.5.2.1.3 the device must have active, up-to-date antivirus and anti-malware protection;
3.5.2.1.4 the device must be protected by secure authentication methods, such as a PIN, fingerprint, or other forms of multi-factor authentication methods;
3.5.2.1.5 Data encryption must be enabled on the device.
3.5.2.2 All sensitive data related to the university (including personal data, research materials, financial records, etc.) must be stored securely on BYOD devices, by implementing appropriate security measures (multi-factor or biometric authentication, strong passwords, encryption, etc.).
3.5.2.3 When using a personal device, the user must adhere to the organisation's security policies and protocols, including installing required management software to ensure compliance with security requirements and control access from the device.
3.5.2.4 Users are responsible for securely backing up the data on their personal devices.
3.5.2.5 If a device is lost or stolen, the user must promptly notify the IT Helpdesk so that appropriate measures can be taken to delete data and revoke access.
3.5.2.6 If a device is blocked from accessing the university's systems due to termination of employment, device replacement, or any other reason, all sensitive and work-related data must be deleted in accordance with the instructions of the Information Technology Services.
3.5.3 Management process:
3.5.3.1 the Information Technology Services provides guidance and advice to ensure security;
3.5.3.2 network traffic and device connections are secured through network segmentation, network security configurations and monitoring.

4. Acquiring, issuing and decommissioning of end-user devices

4.1 Acquiring devices

4.1.1 End-user devices are ordered in accordance with the Public Procurement Rules. Each structural unit submits its device orders to the Information Technology Services, who is responsible for processing and coordinating the orders. The cost of an order is covered by the respective structural unit. The device is entered into the device register managed by the Information Technology Services.

4.2 Deploying gifted or donated devices

4.2.1 If a structural unit wishes to use a device that has been gifted or donated to the university, a corresponding request must be submitted to the Information Technology Services. The IT Helpdesk shall arrange the cleanup, registration and deployment of the device.

4.3 Building and registering a device

4.3.1 If a structural unit wishes to assemble a device from various components, the IT Helpdesk must be notified thereof after the assembly, and they will enter the device in the computer register.

4.4 Selecting a device profile

4.4.1 The Information Technology Services issues devices with the default fully centrally managed Windows user profile, unless the device does not support the default Windows user profile, in which case the conditions specified in clause 3.5 apply). If needed, the structural unit and/or the user can request an alternative profile when placing an order. If the structural unit or the user wishes to change the profile later, the structural unit or the user shall contact the IT Helpdesk, who can make the necessary adjustments.

4.5 Issuing devices

4.5.1 Once a device is delivered, the IT Helpdesk will prepare it according to the specified profile. The preparation process includes installing the operating system, necessary software, and configuring security settings. If the Information Technology Services has installed licensed software with an activation key on a device, the user is not permitted to install the software on another device or transfer it to another user without informing the Information Technology Services. The Information Technology Services must record the changes in the asset management system. After preparation, the device is issued to the end user, along with user instructions and a notification of security requirements.

4.6 Using devices

4.6.1 The Information Technology Services is responsible for the technical management of university's devices, the centralised installation of security patches and software updates, and the maintenance of information security. A structural unit and its employees are responsible for the daily safe use and maintenance of the devices issued or made available to them. Adhering to the following requirements is mandatory to ensure the security and reliability of devices operated by the user:

4.6.1.1 the user must ensure that the devices are safeguarded against physical threats (such as theft and damage) and environmental hazards;

4.6.1.2 the user must keep the devices updated by installing all required security patches and updates. Using unlicensed software is prohibited;

4.6.1.3 the user must use strong passwords and adhere to the university's authentication policies, including two-factor authentication.

4.6.1.4 If users install personal software or make changes that affect device management (such as changes to the device's hostname, user, or software), the Information Technology Services must be notified so that the asset register can be updated accordingly. The notification must include the device's hostname, the end user's name, and details of the software (e.g., name and activation information);

4.6.1.5 users must regularly back up all essential data using the recommended backup solutions;

4.6.1.6 users must adhere to all the university's information security policies and guidelines and promptly notify the Information Technology Services of any security incidents or suspected breaches.

4.7 Decommissioning a device

4.7.1 Cleanup of the device used

4.7.1.1 When the user of a device leaves the university, the respective structural unit must submit a request to the IT Helpdesk to clean the device. The IT Helpdesk deletes all data and profiles linked to the previous user, updates the computer register and makes the necessary changes in the device management software. The cleaned device remains in the possession of the respective structural unit and is recorded in the device inventory list.

4.7.2 Issuing a device to a new user

4.7.2.1 The structural unit may assign the cleaned device to a new user for use. When assigning a device to a new user, the structural unit shall update user details in the computer register. The device will be issued to a new user in accordance with the designated device profile and in compliance with the university's security requirements.

4.8 Permanently removing a device from use and destroying it

4.8.1 The prerequisite for permanently removing a device from use is to clean the device, which includes deleting data and profiles, as well as making the necessary changes in the computer register and device management software. All data on the device shall be securely deleted to prevent any data leakage.

4.9 Scenarios for permanently removing a device from use

4.9.1 Selling and/or donating a device to a third party.

4.9.1.1 A structural unit can decide to sell or donate its devices to a third party (e.g. a departing employee or other party). The selling price of a device is set by the IT Helpdesk, based on the market

value and/or the residual value of the device. Before selling or donating a device, a request must be submitted to the IT Helpdesk for cleaning the device During the cleaning process, all data is deleted, the original operating system is reinstalled, and the corresponding updates are made to the computer register and device management system. The device is then returned to the structural unit, who can either resell it (by issuing a sales invoice) or donate it to a third party, following the procedures established by the university.
4.9.2 Depreciation, damage to and disposal of devices
4.9.2.1 If a device becomes depreciated, is no longer suitable for performing work-related tasks, or is damaged, a request must be submitted to the IT Helpdesk for the device to be cleaned. During the cleaning process, the data on the device is deleted (or the storage drive is removed and sent for separate destruction), the relevant record is deleted from the device management system, and a corresponding entry is made in in the computer register. The IT Helpdesk shall arrange the disposal of the device in compliance with safety and environmental regulations.
4.9.3 Loss or theft of a device
4.9.3.1 The user must immediately notify the Information Technology Services if a device is lost or stolen. The Information Technology Services shall revoke access and ensure remote data deletion, except for unmanaged devices where deletion is not possible. The device record is deleted from the management system, and a corresponding note is made in the computer register.

5. Security, data protection and privacy
5.1 The Information Security Division of the university's Information Technology Services uses a range of automated tools to maintain security and prevent potential threats. These include log analysis, anomaly detection, website and security scans, as well as anti-virus and anti-malware software. All monitoring activities are legal and conducted in compliance with Estonian and EU data protection regulations, including the GDPR. The monitoring activities are proportionate and use the least privacy-intrusive measures possible. The aim is to ensure the security of IT systems and prevent potential security threats. The collected data is used exclusively to ensure system security and prevent potential security threats.

6. Training, notifications and support
6.1 The Information Technology Services:
6.1.1 organises regular information security training for staff and students;
6.1.2 notifies about new threats and vulnerabilities;
6.1.3 provides support and assistance to all users in resolving hardware and software issues on fully centrally managed computers. In other cases, the university's Information Technology Services offer support on a best-effort basis.

7. Supervision
7.1 The implementation of the Rules for the Management and Use of End-User Devices is monitored by the Internal Auditing Office in accordance with its work plan. If any non-compliance is detected, corrective measures are taken and documented.
7.2 Violations of the Rules or non-compliance with information security policies are subject to appropriate sanctions, such as warnings, restriction on access, termination of employment or other legal action.

8. Implementation
8.1 The Rules apply to all new devices issued starting from the date the Rules come into effect. The profiles of devices previously issued to users may not fully match the established procedure. These devices will be gradually updated to align with the established procedure. The Information Technology Services reserves the right to preserve the differences in device settings and configurations that cannot be changed due to technological complexity or economic impracticality. These differences are documented in the asset register.
8.2 The Rules shall be reviewed at least once a year to account for changes in technology, regulations and user needs.