Confirmed
with the Rector of the EKA University of Applied Sciences
order no. 2-16/25/02
from 2025 January 27

INFORMATION SECURITY POLICY

1. General questions

1.1. The purpose of the information security policy (hereinafter referred to as the Policy) is to determine the principles for achieving the security of all information and related technological resources of the EKA University of Applied Sciences (hereinafter referred to as the University), with the aim to:

1.1.1. Protect valuable information resources of the University;

1.1.2. Protect the information of the University employees, students, partners and suppliers;

1.1.3. Ensure availability, integrity, confidentiality of information;

1.1.4. Manage security threats;

1.1.5. Identify and minimize security incidents;

1.1.6. Restore systems operation after security incidents.

1.2. The policy has been developed as a basic document that defines the main basic security conditions for the information technology environment and defines procedures for ensuring the confidentiality, integrity and availability of information and technological resources.

1.3. When developing or correcting the University's internal regulatory documents, the norms and principles established by the Policy must be followed.

1.4. The policy is binding on all employees of the University and its students.

2. Objectives and guidelines of the information security policy

2.1. Provide such an information technology environment that the System (the term "System" includes all University information systems, software and related infrastructure, such as e-mail, e-study environment, Moodle, Office365, Windows operating system, etc.) is protected against external and internal security threats.

2.2. To confirm the support of the management of the University for ensuring information security, in accordance with the University's needs, binding regulatory acts and security norms.

2.3. The information security policy is binding on all users of the System.

3. Information security policy tasks

3.1. Ensure the availability of information (access to information within a certain period of time after requesting information).

3.2. Ensure information integrity (maintaining complete and unchanged information).

3.3. Ensure confidentiality of information (transfer of information only to those persons who are authorized to receive and use it).

3.4. Protect System information resources.
3.5. Protect the technical resources of the System.
3.6. Identify System Security Threats.
3.7. Assess System security risks.
3.8. Detect System Security Incidents.
3.9. Restore System operation after system security incidents.

4. Organizational principles of information security management

4.1. A set of documents and measures, the implementation of which ensures the achievement of the goal of the information security policy, has been determined and is being independently improved at the University.

4.2. The University promotes the understanding of each employee and student about the responsibilities in managing risks and continuity of operations and ensuring the protection of information and technical resources by conducting regular education of the University's employees and students.

4.3. The University ensures constant coordination and monitoring of the implementation of the information security policy.

4.4. In cases where University staff or students do not comply with the requirements of the Policy, the University management may initiate a disciplinary process in accordance with regulatory enactments. In addition, in certain cases, arbitrarily accessing Information Systems, performing malfunctions and other unauthorized actions may be subject to criminal liability, taking into account, for example, Articles 241, 243, 245 of the Criminal Law.

4.5. The University has a clearly defined and understood division of responsibility for information security:

4.6. Rector of the university:

4.6.1. Is responsible for information security;
4.6.2. Determines and approves the information security policy;
4.6.3. Provides the necessary means and support for the implementation, maintenance and improvement of the information security policy;
4.6.4. Determines the division of duties and responsibilities regarding information security:
4.6.4.1. The person responsible for information security management is the Head of the IT department of the University;
4.6.4.2. The manager of the technical resources of the system is the head of the IT department;
4.6.4.3. The manager of the system information resources is the head of the IT department.

4.7. Person responsible for information security management:

4.7.1. Organizes information risk analysis;
4.7.2. Ensures maintenance and implementation of necessary information security documents;
4.7.3. Monitors compliance with established security requirements and investigates security incidents;
4.7.4. Provides training of employees in the field of information security.

4.8. Manager of technical resources of the system:

4.8.1. Is responsible for purchasing, developing, operating and maintaining technical resources of the System;

4.8.2. Ensures the technical and logical protection measures of the System;
4.8.3. Is responsible for managing System access rights;
4.8.4. Takes measures to restore the System operation if the System operation is disrupted.

4.9. The manager of the technical resources of the system:
4.9.1. Is responsible for determining the access control policy for the information resource;
4.9.2. Classifies the information resources under his control;
4.9.3. Defines security requirements for an information resource.

4.10. Users:
4.10.1. Become familiar with and undertake to comply with the requirements of internal regulatory acts in the field of information security;
4.10.2. Report on risks, information security events and incidents identified in the System.

5. Compliance of information security with regulatory acts and standards

5.1. The system complies with the legislation of the Republic of Latvia in the field of information security:
5.1.1. The system complies with the requirements of the laws and regulations of the Republic of Latvia in the field of information technology and information security (including the requirements for the protection of physical personal data).

5.2. The system complies with international regulatory enactments and standards in the field of information security.

6. Principles of information security

6.1. System user accounts:
6.1.1. System users who perform System administration work use special user accounts (hereinafter - System administrator accounts), which are not used for daily operations;
6.1.2. Each user account is associated with a specific natural person;
6.1.3. System accounts are protected in such a way as to prevent users from using them;
6.1.4. Access to the System with an administrator account is only possible using equipment located in the University's controlled premises;
6.1.5. Error messages visible to system users contain only the minimum necessary information - error description and error identifier.

6.2. Password requirements:
6.2.1. Access to the System is protected by a user name and password;
6.2.2. System user passwords are not less than thirteen characters in length and contain at least uppercase Latin letters, lowercase Latin letters, numbers and other symbols;
6.2.3. Every user of the System must change the password after no more than 90 days;
6.2.4. If the system user account password is entered incorrectly five times in a row, this account (except for the System Administrator account) is immediately blocked;
6.2.5. It is forbidden to store and transport system user passwords in unencrypted form, incl. within the user authentication process;
6.2.6. The system user's password is not fully displayed to the user at the time of its entry;
6.2.7. A system user password sent in an unencrypted form over a public data transmission network is single-use;

6.2.8. The System does not have a functionality that allows the System User to save his password so that he does not have to enter it during subsequent connections;
6.2.9. The manager of the technical resources ensures that the equipment, incl. default passwords (installed by the manufacturer or distributor) are not used for the infrastructure equipment that ensures the functioning of the System;
6.2.10. Two-factor authentication (2FA) must be applied to publicly available resources and/or Systems with access to classified data or high security risks.

6.3. Traceability:
6.3.1. Creation and storage of System records is ensured for at least 18 months after the record is made, storing copies of records separately from the System;
6.3.2. System records are created ensuring that the time indicated in the record matches the Coordinated Universal Time (UTC) of the actual event with an accuracy of one second using an NTP server;
6.3.3. The person responsible for System Security Management provides planned monitoring and analysis of the content of System audit logs to detect incidents;
6.3.4. Any access to the System is traceable to a specific System user account or Internet Protocol (IP) address.

6.4. Updates:
6.4.1. The manager of technical resources, in cooperation with the person responsible for information security management, evaluates available software updates and, if necessary, tests them;
6.4.2. All available required software updates must be applied to the system.

7. Information resources

7.1. It is allowed to request only information and data necessary for work functions from the System.
7.2. Viewing, printing, storing the information available in the information resources on your personal computer, on servers or other resources outside the University's data storage area and on other electronic devices or data carriers is prohibited, unless it is provided for by the direct duties of the position or the specifics of the job.
7.3. It is forbidden to connect external data carriers to the work computer. Exceptions are handled on a case-by-case basis, reported through IT Support and approved by the Security Manager.
7.4. It is forbidden to use private data carriers (for example, USB flash drive, external hard drives, etc.). Data carriers may only be used if permission has been received from the Head of the IT department and the data carrier is encrypted and registered with the IT department.
7.5. The system may accumulate information about any actions performed by the user. This information may be used in the investigation of information security violations and other incidents, in compliance with the procedures established by regulatory acts.
7.6. Information should not be stored on a computer's hard drive. The information must be stored in the file storage location specified by the University.
7.7. Private data may not be stored on computers assigned by the University.
7.8. Employees must also adhere to a "clean desk" policy, which means that confidential information is not left unattended and is always securely protected when leaving the workplace.

7.9. For computers, when they are not with the user, the computer or its screen must be locked (English - "Lock computer" with the keyboard key combination CTRL+ALT+DELETE or Windows + L)

8. Information protection measures

8.1. All University-owned end-user equipment that is used on a daily basis to connect to the System includes anti-virus functionality through anti-virus software.

8.2. The functionality of the system is executable with the minimum set of rights possible.

8.3. Physical access to the equipment that ensures the operation of the System is allowed only to persons authorized by the University or accompanied by such persons.

8.4. The flow between the information system and its users, as well as between the information system and other information systems, is controlled using a firewall solution and data encryption.

8.5. During the development and testing of the System, it is not allowed to endanger the integrity of the data stored in the Systems, therefore, the System test environment has been created for such purposes.

8.6. Deploying the system in resources provided by an external service provider is permitted only if the service provider is a legal entity registered in a member state of the European Union or the European Economic Area, and the information stored in the System is located only on the territory of the countries of the European Union or the European Economic Area. In addition, the University ensures supply chain security by continuous analysis, monitoring and control of supply chain risks.

8.7. All Systems important for the activities of the University are ensured continuity and recovery by making regular backup copies and implementing controls for the continuity of the University's activities.

9. Acceptable level of information security risks (availability, integrity and confidentiality risks)

9.1. The person responsible for information security management performs an analysis of information security risks at least once a year.

9.2. As part of the risk analysis, in cooperation with the Head of the University, an assessment is made as to whether the costs of limiting risks and ensuring the continuity of operations are commensurate with the possible losses that could occur in the event of the realization of these risks or the termination of the University's operations.

10. System user registration and its cancellation procedure

10.1. When new employees and academic staff start working legal relations, they must immediately familiarize themselves with the study information systems and related issues before they are granted access to the University Systems.

10.2. The workplace of the system user is equipped with the minimum necessary System resources according to the duties of the work to be performed.

10.3. The request of a new System user is signed by the user's direct manager and approved by the System information resource holder in accordance with the access control policy.

10.4. Each System user is assigned a unique identifier and password, as well as certain access rights.

10.5. The user of the system is responsible for maintaining and not disclosing the assigned identifier and authentication tools.
10.6. It is forbidden to access those System resources to which access rights have not been granted.
10.7. System user registration is cancelled:
10.7.1. When the user terminates employment with the University;
10.7.2. At the request of the user's direct manager;
10.7.3. In case of non-compliance with system security requirements.

11. Rights, obligations, limitations and responsibility of system users

11.1. The user of the system has the right to receive advice from the person responsible for information security management and the manager of the technical resources of the system about the operation of the system and security requirements.
11.2. The System user has the right to use the assigned System information resources only for the performance of work duties.
11.3. The system user is obliged to immediately report to the person responsible for information security management (e-mail andris@augstskola.lv) if:
11.3.1. It is suspected that the authentication tool has been learned/acquired by another person;
11.3.2. Suspicions have arisen about deviations in the operation of the System.
11.4. The system user is obliged to read the messages sent by the system administrator and to perform the indicated actions in time.
11.5. The system user is prohibited to:
11.5.1. Use the information and technical resources of the System to distribute or store non-work related information;
11.5.2. Perform actions that unreasonably burden the information and technical resources of the System;
11.5.3. Unauthorized transfer of information or technical resources of the System to a third party;
11.5.4. Change the System configuration and interfere with the System without authorization.
11.6. The user of the system is responsible for damages caused by non-compliance with the requirements set forth in these regulations.
11.7. The user of the system is responsible for actions performed using his/ her identifier and authentication tool, as well as for damages caused by non-compliance with information security requirements.
11.8. If the user is no longer an employee or student of the University or has been assigned a new position and/or responsibilities at the University, the user's access and authorization must be reviewed.

12. Unacceptable usage claims

12.1. Viewing, creating or transmitting information that is fraudulent or otherwise illegal or inappropriate.
12.2. Sensitive data and confidential data must not be transmitted in an unencrypted form and appropriate security mechanisms must be applied when transmitted.

12.3. Threatening and intimidating users, including any message that could constitute bullying or harassment, such as on the basis of gender, race, disability, religion or belief, sexual orientation or age.

12.4. Use foul or abusive language to incite hatred against any ethnic, religious or other minority group.

12.5. Violate intellectual property rights, including copyright, trademark, patent, design and moral rights; distribute unsolicited advertising known as "spam".

12.6. Forging e-mail messages that purport to come from a specific individual but are actually from someone else.

12.7. Action or omission that intentionally or unintentionally causes a breach of the University's information security, including but not limited to:

12.7.1. Distributing computer viruses or other malicious software;

12.7.2. Attempts to access information for which the user is not authorized;

12.7.3. Use of University Systems for personal commercial business or trade;

12.7.4. Spending a disproportionate amount of time on non-work related sites, such as social media sites;

12.7.5. Unauthorized access, viewing, copying, alteration or destruction of information;

12.7.6. Engaging in activities intended to hide the user's identity;

12.7.7. Sharing or transmitting user accounts, user IDs, passwords, or other mechanisms to others that allow them to access the University's information assets;

12.7.8. Using or unauthorized configuration of software or hardware to knowingly allow unauthorized users to access and obtain unauthorized data;

12.7.9. Use a user's ID, access data, privileges or information that the user is not authorized to use under their current circumstances.

12.8. Attempt to circumvent or subvert the security mechanisms of any System. Users are prohibited from using any computer program or device to intercept and/or decipher access control information.

12.9. Any conduct that may discredit or harm the University, its staff or facilities, or may otherwise be considered intentionally unethical and unacceptable. For example, the following actions will be considered a violation of this Policy:

12.9.1. Viewing, downloading, distributing or storing music, videos, movies, films or other materials for which the user does not have a valid license or other valid permission from the copyright holder;

12.9.2. Distributing and/or maintaining pirated software;

12.9.3. Connecting an unauthorized and/or harmful device to the University network, i.e. which is not configured to comply with the Policy and other relevant University rules and guidelines related to information security;

12.9.4. Bypassing network access controls;

12.9.5. Monitoring and/or interception of network traffic without authorization;

12.9.6. Investigation of System security flaws with methods such as port scanning, etc., without permission;

12.9.7. Connecting any device to network access points, including wireless, for which the user does not have permission;

12.9.8. Non-work-related activities that create a large network traffic, especially those that interfere with other users' use of the Systems or cause financial costs;

12.9.9. Excessive use of resources, such as file storage, causing a denial of service to others;
12.9.10. Using CDs, DVDs and other storage media to copy unlicensed software, music, etc.;
12.9.11. Copying material from other people's websites without the express permission of the copyright holder;
12.9.12. Use of peer-to-peer network and related software.

12.10. Cases of unfair use of the University System will be subject to disciplinary procedures and in some cases criminal liability may be appropriate.

12.11. It is forbidden to store passwords in an unencrypted form, in a freely accessible and visible place.

12.12. If the University's network is used to access another network, any abuse of that network's acceptable use requirements will be considered an unacceptable breach of the University's network use requirements.

12.13. Periodically, the University's IT department may implement technical measures to monitor activities on the University's network in order to ensure compliance with the requirements of this Policy and to conduct inspections for security purposes.

13. System user support procedure

13.1. The University provides the technical and informational resources of the System necessary for the user's work duties.

13.2. The University provides information to the user about:
13.2.1. System operation;
13.2.2. System operation planned interruptions;
13.2.3. Action during unplanned System interruptions.

13.3. System user support contact information (e-mail: andris@augstskola.lv).

14. Procedure for using the system

14.1. Access to the Study Information Systems is possible only by authorization using the University's website (https://www.augstskola.lv), otherwise the device will be blocked by authorization in other ways.

14.2. The system is used to perform tasks and functions of the University.

14.3. The system is used during the working hours of the University, using funds allocated by the University.

14.4. All user activities in the System can be monitored, and the obtained data can be used to ensure control of the performance of work duties and general information security at the University.

15. Security of portable computers

15.1. Data must not be stored on the laptop hard drive, but must be stored on the University's file server.

15.2. Laptop Security:
15.2.1. The preparation of the portable computer for work is provided by the IT support service of the University;
15.2.2. The user ensures that laptops or mobile devices are not left unattended, for example, when travelling, ensure that laptops are stored safely;

15.2.3. User shall ensure that laptops are not left unattended in non-secure areas such as meeting rooms adjacent to public access areas and hotel rooms where others may have access. The user must use laptop computer locks and/or close the door when leaving the work space;

15.2.4. The user is aware of the potential for opportunistic or targeted laptop bag theft in busy public areas, including airports, train stations, hotel lobbies, showrooms, etc., and on public transportation such as buses and trains. When traveling, avoid placing laptops in places where they can be easily forgotten or left behind, such as taxi seat pockets. Be aware that using a laptop in public places is likely to attract the attention of those nearby. It is possible that the information displayed on the screen of a portable computer may lead to unauthorized disclosure of this information, therefore it is not recommended to process confidential information in public places or use appropriate privacy filters for the screen;

15.2.5. Ensure that timely software and operating system updates are always performed as soon as they become available.

16. Mobile Device Security

16.1. Requirements for mobile devices should include physical protection and access control, cryptographic techniques (data encryption), backups and anti-virus protection where technically feasible.

16.2. The user takes into account good practices to set additional security and privacy settings for mobile devices, such as:

16.2.1. Unlock the mobile device with a pin code or fingerprint or other biometric means;

16.2.2. If available, sets the "find my phone" functionality and the possibility to remotely delete data and block the mobile device;

16.2.3. User must check and review app permissions;

16.2.4. Advertising and opting out of “ad-tracking” ads and location tracking to prevent ad networks from building based on personal likes and dislikes based on viewing, reading or other habits;

16.2.5. Reduce/disable phone sleep timeout and auto-lock after a certain period of time;

16.2.6. Block lock screen notifications to prevent others from seeing personal content, even if the PIN code for the mobile device is not known;

16.2.7. Prevent the installation of unauthorized applications: the way to ensure this is to have only verified applications installed on the phone, ensuring that the possibility of unknown sources is excluded; as well as periodically checking for software updates;

16.2.8. Ensure timely software and operating system updates are always performed as soon as they become available.

17. Bring your own device (BYOD) requirements

17.1. The University allows the use of personally owned devices under the following conditions:

17.1.1. All personally owned laptops, workstations, cell phones or other devices must have approved virus and spyware detection/protection software along with personal firewall protection;

17.1.2. Devices that have access to University email must have a PIN or other secure authentication mechanism enabled;
17.1.3. Confidential information may only be stored on devices that are encrypted in accordance with the University's information security policy;
17.1.4. It is preferable to use the CERT.LV DNS firewall (more information is available at https://dnsmuris.lv);
17.1.5. Theft or loss of any device used to create, store or access confidential information must be immediately reported to the Information Security Manager;
17.1.6. All devices must have updated software and operating system versions;
17.1.7. "Jail-broken" or rooted devices may not be used to connect to University information resources.

17.2. The University reserves the right to cancel the right to use a personally owned device in case users do not comply with the requirements set out in this Policy.

17.3. Use cases for own devices also include the above requirements in the mobile device and laptop security sections.

18. Use of Internet and electronic mail

18.1. It is allowed to use the electronic mail of the University only for work and/or study purposes and it is forbidden to indicate it as private contact information on various internet portals or other public websites.

18.2. Users may not use the University e-mail for personal needs or personal gain.

18.3. Users may not download software from the Internet or execute or accept any software or other code over the Internet unless it is in accordance with University policies and procedures.

18.4. It is forbidden to open e-mail attachments received from unknown sources and Internet address links specified in e-mails. The fact of receiving such an e-mail must be immediately reported to the IT support service.

18.5. The user, upon receiving an e-mail and having doubts about a possible computer virus, must immediately notify the IT support service.

18.6. It is forbidden to resend an e-mail if a notification has been received that the addressee cannot receive the message due to exceeding the e-mail server's limit.

18.7. The size of one e-mail cannot exceed 20 megabytes (hereinafter - MB).

18.8. To exchange large files, use the University's file exchange service https://augstskola.sharepoint.com.

18.9. By regularly deleting unnecessary information, the e-mail user must ensure that the size of his mailbox on the server does not exceed 7 GB. The IS administrator may block the user's e-mail account if the total volume of the mailbox exceeds the specified volume.

19. Software and information systems

19.1. Only licensed and authorized software is allowed to be used for work and study duties. Installation and use of unlicensed or private software on University computers is prohibited.

19.2. It is forbidden to independently install or remove software on University equipment without the written permission of the Head of the IT department.

20. System security criteria

20.1. The system is available continuously.

20.2. Conditions under which routine procedures are replaced by crisis management procedures:

20.2.1. If the System operation recovery time exceeds the permissible;

20.2.2. If data loss is detected in the System.

21. Closing questions

21.1. The policy is reviewed at least once a year, as well as in the following cases:

21.1.1. If changes to the System may affect the security of the System;

21.1.2. If new System security threats have changed or been discovered;

21.1.3. If the number of System Security incidents increases or a significant System Security incident has occurred.

21.2. If, upon reviewing the policy, a relevant need is identified, update it.

21.3. If changes in the organizational structure of the University affect the system security management organization.

21.4. If the names of the processes, the names of the structural units of the University, the responsible employees, their positions, workplace addresses, telephone numbers, etc., the internal regulations of the University have changed, as well as references and links to other related documents, they are not considered amendments to the document. .

21.5. If significant changes are made to the content of the document and the actions described in it, the amendments are approved by the management of the University.

21.6. The information security manager is responsible for updating the Policy.