INFORMATION SECURITY POLICY

(staff)

APPROVED
30 August 2022

Acting Rector of RISEBA:
Prepared
by: Head of the IT Department
Data Protection Specialist

Contents

1. DEFINITIONS

RISEBA	SIA "RISEBA University of Applied Sciences" (reg. No. 40003090010), its structural units, branches, representative offices, affiliated companies and associations.
Management	Rector of RISEBA; Vice-Rector for Academic Affairs; Vice-Rector for Science; Vice-Rector for Development; Director Of Finance; Administrative Director
Immediate Supervisor	RISEBA representative, an employee who is specified in the relevant employee's employment contract or appointed by a RISEBA Order as the direct manager of the employee and/or the head of the department.
Employee	Any person with whom RISEBA has an employment relationship.
DPO	RISEBA data protection specialist, dpo@riseba.lv
Resource Holder	RISEBA IT Department
Policy	This RISEBA Information Security Policy
Third party	A natural person, legal entity, public authority, agency or body other than the data subject, the controller, the processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Cooperation partners	Suppliers, clients, students, invited specialists, external faculty members, service providers, etc.
RISEBA account	Any account assigned to an Employee, maintained by RISEBA and to which the Employee is granted access upon entering into an employment relationship with RISEBA. Example: email, SharePoint, MyRISEBA, eRISEBA, etc.
Information	Data, including personal data, held by RISEBA, which includes, but is not limited to, confidential, restricted-access and internal-use information.
RISEBA devices	All devices intended for the processing, storage and transmission of information and data (including desktop computers, laptops, tablets, smartphones and other handheld devices) owned by RISEBA.
RISEBA premises	Premises owned by RISEBA or leased by RISEBA, which are provided with physical security and access control.
User	A person who has created a RISEBA account and has been granted access to RISEBA information.

2. Policy OBJECTIVE AND DESCRIPTION

2.1. The objective of the Information Security Policy is to ensure the implementation and maintenance of RISEBA information system management that guarantees the continuous security of RISEBA information systems and protects RISEBA information assets from unauthorised access and misuse.

2.2. This Policy applies to the processing of information and data in any systems and using any data storage media involved in data/information processing, regardless of whether the data/information processing takes place within the framework of an employment relationship with RISEBA or in relations with third parties.

2.3. This Policy also sets out how RISEBA employees use the equipment and tools available to them to perform their work duties.

2.4. This Policy may apply in conjunction with all other Policies, provisions, Orders and guidelines adopted and implemented by RISEBA.

2.5. All information security systems and information security issues not covered by this Policy must be addressed to the Resource Owner and DPO.

2.6. Employees are obliged to comply with this Policy, as well as with the provisions of applicable Latvian or international legislation governing the processing and protection of information. Failure to comply with the provisions of this Policy and other data protection regulations is considered a serious breach of work discipline and, at RISEBA's discretion, may constitute grounds for the imposition of disciplinary sanctions or the dismissal of the Employee, and may also result in administrative or criminal liability.

3. PERSONAL DATA PROTECTION

3.1. All personal data and other information that can be used to identify data subjects shall be collected and processed only where there is a legal basis for such processing of personal data and to the extent necessary for the performance of the Employee's duties, provided that such activities are carried out within the scope of the powers granted to the Employee and in accordance with the data protection provisions laid down by law.

3.2. Consequently, the provisions of the internal personal data processing Policy must be strictly observed, and measures must be implemented that specifically comply with the principles of data protection by design and data protection by default.

3.3. The processing of data subjects' requests and complaints, as well as the preparation of responses, is carried out by RISEBA DPO. Upon receiving a data subject's request or complaint regarding their personal data, the Employee shall immediately inform the DPO of such a request, attaching a description of the situation as well as other information related to the specific personal data.

4. SYSTEMS USED FOR DATA AND INFORMATION PROCESSING

4.1. Any information systems, including but not limited to computer hardware, any type of software, cloud platforms and services, operating systems, any data storage media, network accounts, email accounts, browsing systems and any other technical infrastructure and tools used by RISEBA, are considered the property of RISEBA.

4.2. All Employees must use the technical equipment and tools referred to in clause 4.1 with due care and attention, and solely for purposes related to RISEBA's operations. The only exception is where RISEBA has provided the Employee with technical equipment (e.g. a mobile phone) and has expressly permitted its use for private purposes as well.

4.3. All systems, software and equipment used by RISEBA must be properly licensed and lawfully acquired.

4.4. RISEBA regularly (at least once a quarter) checks and updates the systems and software used for information data processing to ensure the continuous security and integrity of all RISEBA information technology systems, as well as ongoing compliance with and enforcement of this Policy and applicable legal requirements.

4.5. RISEBA appoints a system *owner* for each information system.

4.6. The system owner is responsible for:

- The availability, integrity and confidentiality of information systems;
- Coordinating and managing the acquisition, development, modification and operation of information systems;
- The implementation and ongoing maintenance of information systems;
- Maintaining communication with the information system supplier;
- Determining and regularly reviewing access rights to information systems;
- Organising and supervising the process of securing the financial resources necessary for the implementation and maintenance of information systems (e.g. for the purchase or renewal of licences, the purchase of support services, or the subscription to outsourced services).

5. SECURITY MEASURES WHEN PROCESSING DATA AND INFORMATION

5.1. This Policy, as well as regulatory acts setting out data security requirements, applies to all forms of information (in paper format, electronic form, etc.) and all methods of processing (data collection, processing, protection, storage, etc.).

5.2. Employees are responsible for ensuring that RISEBA data in their possession is managed securely. All data must be stored on RISEBA devices, servers, accounts or in accessible environments (e.g. SharePoint, OneDrive, network drive). To store RISEBA data in other storage locations, explicit, written permission from the Resource Holder is required.

5.3. Staff are obliged to always keep an eye on devices and data storage media used for work purposes, and to store them in a secure place. When devices are not in use or are left unattended, they must be password-protected or switched off, whilst data storage media must be placed in a secure storage facility.

5.4. Data processed electronically outside RISEBA's premises or the secure data centre of a partner organisation, and which is not considered freely accessible public information, must be encrypted at all stages of processing.

5.5. Employees are prohibited from using their private or other organisations' email accounts for communication related to RISEBA's activities, nor may they forward any information related to RISEBA's activities to their private or other organisations' email accounts and/or cloud platforms which the Employee uses privately or for work unrelated to RISEBA.

5.6. Where there are no sufficient legitimate grounds for continuing data processing, the data shall be deleted, all copies shall be destroyed, and the relevant Employees shall be informed that the data in their possession must be destroyed or returned to RISEBA, particularly if the Employee's employment relationship is terminated.

6. ACCESS MANAGEMENT

6.1. Any access rights granted to Employees are assigned taking into account their job duties and based on the 'need-to-know' principle. Access to any RISEBA system does not imply that the Employee is authorised to view or use all the information contained in such a system.

6.2. Upon receiving access details for RISEBA systems (username and temporary password), the Employee is obliged to change the password immediately after logging into the system for the first time.

6.3. If logging into RISEBA information systems takes place outside RISEBA premises and, where the system provides for such a possibility, the Employee must authenticate themselves in the electronic environment using a two-factor authentication system.

6.4. Employees' system access credentials are unique and identify a specific Employee. Each Employee is responsible for all activities associated with their personal identification accounts, therefore their primary duty is to ensure that access credentials are not accessible to any third party, nor to other Employees or persons, except where RISEBA or the Employee's Line Manager has specified otherwise.

6.5. System security password requirements:

6.5.1. Employees must use passwords that are not easily guessed:

- passwords must not contain the Employee's personal data;
- minimum number of characters – 8, minimum number of uppercase letters – 1, minimum number of special characters – 1;
- passwords must not be reused.

6.5.2. The resource owner must ensure:

- that Employees are required to change their passwords for the systems at least once every 3 months;
- automatic verification of password complexity and compliance with the provisions set out in clause 6.5.1;
- distinguishing between upper and lower case letters in passwords.

6.6. If the maximum number of failed access attempts exceeds 5 times in a single calendar day, access to the account will be automatically blocked. Only the Resource Holder has the right to unblock the account. The aforementioned controls apply regardless of whether the access attempt is made on a local data transmission network or a public data transmission network.

6.7. Each Employee is personally responsible for ensuring that their security passwords comply with this Policy and all other RISEBA access data security provisions.

6.8. On a regular basis, but at least once a year, the Resource Holder reviews the user rights for RISEBA information systems, as well as whenever:

- the employment relationship with the Employee is terminated, the Resource Holder shall revoke that User's access rights to RISEBA's information systems. Upon revoking an Employee's user rights, the Resource Holder shall ensure that the Employee's manager has access to the Employee's email account previously managed by that Employee.
- in cases where Employees are ordered to take other positions.

7. USE OF RISEBA AND PERSONAL DEVICES. REMOTE WORK.

7.1. When performing work duties on RISEBA premises, the Employee must use RISEBA devices for data processing. Such devices typically include, but are not limited to, a desktop computer, laptop, smartphone or tablet with which the Employee can connect to RISEBA's servers and network. In cases where an Employee works remotely, Employees are permitted to use personal devices to work with RISEBA data only if the requirements of clauses 7.3 and 7.4 of this Policy are met.

7.2. If several Employees request the allocation of RISEBA devices for remote working, but the Resource Manager does not have a sufficient number of devices available, priority is given to administrative staff whose work involves a larger volume of data to be processed, and only then to Academic staff members.

7.3. RISEBA devices used by Employees for work purposes must meet the following requirements:

7.3.1. Only licensed and authorised software may be installed and used on devices; the necessity of such software must be assessed and approved by the Resource Holder before downloading or installing it on devices.

7.3.2. Software installed on devices must be regularly updated to prevent malfunctions and vulnerabilities. If the software developer no longer provides support for the software, its use is not permitted without a risk assessment carried out by the Resource Holder in conjunction with DPO, with the necessary documentation being drawn up.

7.3.3. If the device is a smartphone or tablet/laptop:

- The device must have a password (or equivalent) lock function.
- The password (or equivalent solution) must always be enabled.
- The tablet must have active and up-to-date protection against viruses and malware. Where possible, this requirement must also apply to smartphones.
- The remote location tracking function must be enabled on the device.
- Data and information must be stored in encrypted form.

7.3.4. If the device is a desktop computer:

- Access to the device must be password-protected (or an equivalent solution).
- The password (or equivalent solution) must always be enabled.
- The device must have up-to-date protection against viruses and malware.

7.3.5. If the device is any other type of device:

- Access to the device must be password-protected (or an equivalent solution).
- Data and information must be stored in encrypted form. If the device is not capable of encryption, the information must be encrypted before being transferred to the device.

7.4. All devices used by the Employee for processing RISEBA information and which are not the property of RISEBA must be approved by the Resource Holder. The use of devices belonging to other organisations is not permitted.

7.5. In cases where an Employee uses personal devices to access RISEBA servers and the network, the Employee is obliged to comply with the requirements of this Policy, which shall apply to the Employee's devices as if they were owned by RISEBA, and must also comply with the following requirements:

7.5.1. If the device allows for it, all RISEBA data must be stored separately from other data, in a folder with individual encryption and/or individual password protection.

7.5.2. RISEBA data must be deleted from the device when its storage is no longer necessary for the performance of a specific work task.

7.6. If an Employee receives a notification that a virus has been detected on the device they are using, it is strictly forbidden to access any file on the device, as well as to close any open windows or notification windows, and the Employee must immediately contact the Resource Holder and inform them of the incident.

7.7. The Resource Holder must be informed immediately of the loss of a RISEBA device or a personal device used for the performance of work duties. If the device contained personal data, this must also be reported immediately to the DPO.

8. PROCEDURE FOR THE STORAGE AND DISPOSAL OF DATA STORAGE MEDIA

8.1. Employees are prohibited from using their own private electronic data storage devices or those belonging to another organisation for the storage or transfer of RISEBA data (e.g. memory cards, external/removable hard drives, flash drives/USB drives, CDs).

8.2. RISEBA confidential data may only be stored on electronic media that are password-protected and encrypted.

8.3. When the information contained on RISEBA data storage devices is no longer required, it must be deleted from the electronic data storage device immediately.

8.4. When RISEBA electronic data storage devices are broken or no longer function properly, the data storage devices must be destroyed.

8.5. If RISEBA electronic data storage devices are accessible to several Employees, or if the data storage devices are handed over for use by other persons, the Employee handing over the data storage device must ensure that it does not contain any RISEBA information and may only hand it over for use by another person after the data contained therein has been deleted.

9. RESOURCE SECURITY

9.1. Server security (applies to the Resource holder)

9.1.1. Server equipment used for the storage and processing of RISEBA data must be located in designated RISEBA premises or in the secure data centre premises of a cooperation partner. Physical access to server equipment and the premises where it is located is permitted to the Resource Holder and/or the technical support staff of the cooperation partner under the supervision of the Resource Holder and/or in accordance with the terms of the cooperation agreement;

9.1.2. Access to the server management interface is permitted only via administration accounts specifically designated

for this purpose;

9.1.3. All instances of access to server resources and/or the management interface must be recorded in an audit log, noting the date and time of access, the person or user account that performed the access, and the type of access (viewing, changes, etc.). When making configuration changes, the reason for the changes must be recorded in the log;

9.1.4. Backups of server data and configuration must be performed regularly. At least two copies must be created for each data item, which must be stored physically separate from one another.

9.2. **Network security**

9.2.1. Only RISEBA staff may connect to RISEBA's internal closed WiFi network. Visitors, partners, non-core lecturers and students must connect to the open guest WiFi network to use the internet.

9.2.2. When working remotely, RISEBA provides staff with the ability to connect to RISEBA systems using the SSL VPN system.

9.2.3. Employees are strictly prohibited from using public internet connections (e.g. in internet cafés, libraries, etc.) to access RISEBA data, except in cases where work duties are being performed on a business trip or where there is a critical and urgent work-related necessity and the Employee's Line Manager has provided clear written consent for such action. In all other cases, a mobile network must be used.

9.2.4. When using RISEBA devices, browsing for the Employee's private purposes is permitted, except for playing online games or gambling, sharing data, and viewing websites with prohibited content such as pornography, weapons, terrorism, extremism, and other sites of a negative nature. In implementing information system security management, RISEBA may analyse internet data traffic to detect attacks on the network.

9.3. **Fire safety**

9.3.1. RISEBA provides and maintains fire prevention and detection equipment/systems that operate from independent power sources.

9.3.2. Only gas or powder fire extinguishers are used in data centres, server rooms and rooms housing computing equipment.

9.4. **Temperature and humidity control**

RISEBA ensures appropriate temperature and humidity levels in rooms housing information systems infrastructure and monitors temperature and humidity levels.

10. PROHIBITED ACTIVITIES

10.1. Except where permitted by RISEBA, under no circumstances may equipment, systems or tools belonging to RISEBA or its partners be used for purposes unrelated to the Employee's work duties or unrelated to RISEBA's operations.

10.2. It is strictly prohibited to engage in the following activities:

(a) Infringing the rights of any person or company protected by intellectual property rights, including, but not limited to, the installation, copying, distribution or storage of any illegal software, online platforms, any other electronic content for which RISEBA has not been granted a licence under a specific agreement, on any RISEBA systems or equipment;
(b) Unauthorised copying of copyrighted material;
(c) To infringe the rights of any data subject by excessively and unnecessarily collecting and processing that data subject's personal data;
(d) Access data, a server or an account for purposes unrelated to the performance of RISEBA's activities or the performance of the Employee's duties;
(e) Export software, technical information, encryption software or technology in breach of applicable international or national laws and provisions and/or RISEBA's instructions;
(f) Disclose an Employee's access credentials to RISEBA systems and allow other persons to use their personal account (including, but not limited to, the Employee's family members);
(g) Offer fraudulent or self-serving products or services from a RISEBA account;
(h) Causing a security breach or disruption to network communications. Such security breaches include, but are not limited to: accessing data not intended for the Employee's disclosure, or the Employee logging in to or accessing a server or account without specific authorisation, unless such duties form part of the Employee's job responsibilities or access rights are granted to the Employee in connection with a specific RISEBA project;

(i) Using any programme/script/command or sending any type of message with the aim of disrupting or disabling a user's session.

11. REPORTING AND HANDLING OF SECURITY BREACH INCIDENTS

11.1. Employees must immediately report all data processing security incidents or incidents that may result in breaches of RISEBA's data processing security to both the Resource Holder and DPO.

11.2. The Resource Holder and DPO shall organise all necessary measures to prevent any potential breach or loss, or to mitigate its consequences and restore the previous security status, involving other employees and Management where necessary.

11.3. The Resource Holder and DPO are obliged to ensure timely reporting of information security breaches in accordance with the provisions of Latvian and EU legislation.

11.4. RISEBA investigates and documents every information system security incident. The information system security incident documentation maintains a record of each incident, its status, and other relevant information necessary to investigate the causes of the incident.

11.5. Security breach incidents are handled, including incident identification and analysis, mitigation and recovery. The experience gained is documented and used in training and testing exercises.

12. INCIDENT RESPONSE PLAN

To respond appropriately to incidents, the Resource Holder ensures the development, implementation, maintenance and regular review of an incident response plan. The incident response plan must be updated as necessary.

13. MANAGEMENT AND REPORTING

13.1. The Resource Owner is responsible for:

1. managing information system security and overseeing the maintenance of the Policy, ensuring measures that promote the security, integrity and confidentiality of RISEBA's information systems, regularly reviewing and utilising the latest technological advancements, as well as making full use of available resources;
2. maintaining and updating the Policy, in consultation with the DPO. The Policy shall be reviewed regularly and at least once a year, as well as whenever RISEBA changes, supplements, amends or otherwise modifies existing IT resources and systems;
3. Risk assessment and internal audit. These activities must be carried out in conjunction with the DPO as necessary;
4. security breach prevention and incident management;
5. logging security breaches and recording them in the information systems security incident register.

13.2. Before handing over an information system or its components for technical maintenance or repair, the Resource Holder shall check whether they contain confidential information or personal data. If they do, every possible measure must be taken to ensure the confidentiality of the information (e.g. encryption, anonymisation).

13.3. Following maintenance or repair work, the Resource Holder shall check all potentially affected security controls to verify their operation. In the event of damage to data storage media, it must be ensured that data cannot be recovered from the media and that, in the event of repair, the data will not fall into the hands of third parties.

13.4. The Resource Holder shall maintain communication with persons providing information system security maintenance services and shall ensure that such persons are bound by non-disclosure obligations where such personnel require access to confidential information.

13.5. When conducting a routine data protection compliance audit, the DPO shall request, and the Resource Holder shall be obliged to provide, all information necessary for the DPO to assess whether the objectives of the Policy are being met and whether there is ongoing compliance with the provisions of the Policy. The DPO compiles the information obtained, together with other data protection compliance information, and submits it to the Rector of RISEBA at least once a year.

14. STAFF TRAINING

14.1. The Administrative Director organises regular – at least once a year – staff training on cyber security, which includes, but is not limited to:

- information on the risks and types of online fraud, prohibited activities and other relevant information in the field of

information security, which promotes employees' understanding and safe working practices with RISEBA devices and systems;

- basic knowledge required to ensure the security of information systems and that Employees behave in accordance with
- RISEBA's security requirements, which, among other things, helps to identify and respond to suspicious security incidents;
- information necessary for the implementation of security processes and which complies with the provisions of the Policy.

14.2. Information regarding training shall be documented and retained for 7 years.

15. FINAL PROVISIONS

15.1. The Policy shall enter into force on the date of its approval. It is the duty of management and the Line Manager to ensure that the Employee has familiarised themselves with the provisions of the Policy. Unless otherwise provided for by law, Employees shall be provided with this Policy electronically or in paper form, and it shall be deemed that the Policy has been made available to the Employee, the Employee has familiarised themselves with its provisions, and the Policy is binding on the date of receipt (the moment of receipt of the relevant email, notification via another electronic medium, or provision of the Policy in paper form).

Document classification: RISEBA confidential information					
Title:	RISEBA Information Security Policy				
Responsible person:	Head of the IT Department	**Document approved by:**	Acting Rector of RISEBA		
		Document coordinated by	Data Protection Specialist		
Status:	Valid	**Version:**	1.0	**Date:**	30 August 2022