# INFORMATION SECURITY PROVISION

Students

(Appendix 2 to the RISEBA Information Security Policy)

APPROVED
30 August 2022

Acting Rector of RISEBA:

Prepared by:

Head of the IT Department

# Contents

## 1. DEFINITIONS

| | |
|---|---|
| **RISEBA** | SIA "RISEBA University of Applied Sciences" (reg. No. 40003090010), its structural units, branches, representative offices, affiliated companies and associations. |
| **DPS** | RISEBA data protection specialist, dpo@riseba.lv |
| **Data Controller** | RISEBA IT Department |
| **User** | A student with whom RISEBA has concluded a Study Agreement or another type of agreement, on the basis of which the person participates in studies or training programmes implemented by RISEBA. |
| **Third party** | A natural person, legal person, 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 the processor, are authorised to process personal data. |
| **Provision** | These RISEBA Information Security Provisions |
| **RISEBA account** | Any account assigned to a User, maintained by RISEBA, and to which access is granted to a person upon entering into a contractual 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 and tablets) owned by RISEBA. |
| **RISEBA premises** | Premises owned by RISEBA or leased by RISEBA, which are provided with physical security and access control. |
| **RISEBA data** | Any data, including personal data, which is collected, processed and managed by RISEBA, as well as new data generated through the processing and use of such data. |
| **Personal data** | any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as the person's name, surname, identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |

## 2. PURPOSE AND DESCRIPTION OF THE PROVISIONS

2.1. The purpose of the Provision is to ensure the implementation and maintenance of RISEBA information system management, which ensures the continuous security of RISEBA information systems and protects RISEBA information assets from unauthorised access and misuse.

2.2. The Provision 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 such processing takes place within the framework of RISEBA studies or in relation to third parties.

2.3. The Provision also sets out how RISEBA Users are to use the equipment and tools available to them whilst studying at RISEBA.

2.4. These Provisions may apply in conjunction with all other Policies, Regulations, Orders and Guidelines adopted and implemented by RISEBA.

2.5. All information security systems and information security issues not covered by these Provisions must be addressed to the Resource Holder and DPS.

2.6. Users are obliged to comply with these Provisions, as well as with the requirements of applicable Latvian or international legislation governing the processing and protection of information.

## 3. INFORMATION PROCESSING

3.1. Any information system, 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 owned by RISEBA must be used by the User with due care and attention and solely for purposes related to RISEBA's operations.

3.2. Any information or RISEBA data that becomes available to Users whilst studying at RISEBA and using RISEBA devices is considered to be RISEBA information, to which RISEBA holds the property rights. Consequently, this information is subject to special protection in accordance with these Provisions, applicable legislation on the protection of confidential information, trade secrets and personal data, and must not be disclosed to third parties until RISEBA announces that such information has become public or has otherwise been reclassified as information no longer subject to the protection provisions of these Terms.

3.3. RISEBA data is subject to protection regardless of whether such information has come into the User's possession in printed materials, orally, on data carriers or in audio/video materials, etc.

3.4. If the User is unsure or the available RISEBA data is public data, it must be treated as confidential information.

## 4. SECURITY MEASURES WHEN PROCESSING DATA AND INFORMATION

4.1. These Provisions, as well as regulatory acts setting out data security requirements, apply to all forms of information (in paper format, electronic form, etc.) and methods of processing (collection, processing, protection, storage, etc.), and Users are responsible for ensuring that RISEBA data in the User's possession is managed securely, including in compliance with the requirements of the General Data Protection Regulation.

4.2. Users are obliged to always keep an eye on the devices used for study purposes (hereinafter – Devices), as well as to store them in a secure place. When not in use or left unattended, Devices must be protected with a password or switched off.

4.3. Due to the high security risk, Users are advised not to use public internet connections (e.g. in internet cafés, libraries, cafés, etc.) to access RISEBA accounts and, where possible, should endeavour to use the device's mobile network.

4.4. When using RISEBA devices, browsing for the User'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.

## 5. ACCESS MANAGEMENT

5.1. Upon receiving access details for RISEBA systems (username and temporary password), the User is obliged to change their password immediately after their first login to the system.

5.2. Users' system access credentials are unique and identify a specific User. Each User is responsible for all activities associated with their personal identification accounts; therefore, their primary duty is to ensure that access details are not made available to any Third Party or other persons, except where RISEBA has specified otherwise.

5.3. System security password requirements:

5.3.1. The User must use passwords that are not easily guessed:

- passwords must not contain the User'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.

5.4. If the maximum number of failed login 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.

5.5. Each User is personally responsible for ensuring that their security passwords comply with these Provisions and any other RISEBA access data security provisions, if such have been made known to the User.

## 6. USE OF PERSONAL DEVICES.

6.1. Devices used by Users to log in to RISEBA accounts must meet the following requirements:

6.1.1. Only licensed and authorised software may be installed and used on the devices;

6.1.2. Software installed on devices must be regularly updated to prevent malfunctions and vulnerabilities;

6.1.3. The device must have a password (or equivalent) lock function;

6.1.4. The password (or equivalent solution) must always be enabled;

6.1.5. The device must have enabled and up-to-date virus and malware protection.

6.2. The use of devices belonging to other organisations is not permitted.

6.3. If the User receives a notification that a virus has been detected on the device they are using, it is strictly forbidden to access any RISEBA account; the User must close any open windows or notification windows and immediately contact the Resource Holder to report the incident.

## 7. PROHIBITED ACTIVITIES

7.1. It is strictly prohibited to carry out 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;
(b) Copying copyrighted material without permission;
(c) infringe the rights of a data subject by collecting and processing that data subject's personal data in an excessive manner and without a legitimate basis;
(d) access a RISEBA account for purposes unrelated to studies or other obligations arising from the study contract;
(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 the User's access details to RISEBA accounts and systems and allow other persons to use the personal RISEBA account (including, but not limited to, the User's family members);
(g) Offering fraudulent or self-serving products or services via 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 User's disclosure, or logging in or accessing a server or account without specific authorisation, unless access rights are granted to the User in connection with a specific RISEBA project;
(i) Using any programmes/scripts/commands or sending any type of messages with the aim of disrupting or disabling another user's session.

## 8. REPORTING AND HANDLING OF SECURITY BREACH INCIDENTS

8.1. The User 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 DPS.

## 9. FINAL PROVISIONS

9.1. These provisions form an integral part of the RISEBA Information Security Policy. Unless otherwise provided by law, Users shall be made aware of these provisions electronically or in paper form, and it shall be deemed that the Provision has become available to the User, the User has familiarised themselves with it, and the Provision becomes binding on the date of receipt (the moment of receipt of the relevant email, notification in another electronic environment, or provision of the Provision in paper form).

| | | | | | |
|---|---|---|---|---|---|
| **Document classification:** RISEBA confidential information | | | | | |
| **Title:** | RISEBA Information Security Provision (Appendix No. 2) | | | | |
| **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 |