INFORMATION SECURITY PROVISION

(invited specialists and non-core lecturers)

(Appendix 1 to the RISEBA Information Security Policy)

APPROVED

30 August 2022

Acting Rector of RISEBA:

Prepared by:

Head of the IT Department

Data Protection Specialist

Contents

1. DEFINITIONS

RISEBA	SIA "Biznesa, mākslas un tehnoloģiju augstskola "RISEBA""(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
DPS	RISEBA Data Protection Specialist, dpo@riseba.lv
Resource holder	RISEBA IT Department
Provision	These RISEBA Information Security Provisions
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.
Cooperation partners	Suppliers, clients, students, invited specialists, external faculty members, service providers, etc.
RISEBA account	Any account assigned to a User, which is maintained by RISEBA and to which access is granted upon entering into a contractual relationship with RISEBA. Examples: 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.
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.
User	A person who has created a RISEBA account and has been granted access to RISEBA information (e.g. invited specialists, Non-core lecturers).

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. These Provisions apply to the processing of information and data in any systems and using any data storage media involved in the processing of data/information, regardless of whether the processing of data/information takes place within the context of RISEBA 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 in order to fulfil their contractual obligations.

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. PROTECTION OF PERSONAL DATA

3.1. All personal data and other information that can be used to identify data subjects may be collected and processed only where there is a legal basis for such processing of personal data and to the extent necessary for the fulfilment of the User's contractual obligations

, provided that such activities are carried out within the scope of the authority granted to the User and in accordance with the data protection provisions laid down by law.

3.2. Consequently, the provisions on the processing of personal data, which have been made known to Users in the agreement concluded between RISEBA and the User or in its Appendices, must be strictly observed, and measures must be implemented that comply, in particular, with the principles of data protection by design and data protection by default.

4. SYSTEMS USED FOR DATA AND INFORMATION PROCESSING

4.1. Any information systems, including but not limited to computer hardware, software of any kind, 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.

5. SECURITY MEASURES WHEN PROCESSING DATA AND INFORMATION

5.1. 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 its processing methods (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.

5.2. Users are obliged to always keep an eye on the devices and data storage media used for the purposes of fulfilling the contractual relationship (hereinafter – Devices), as well as to store them in a secure place. When not in use or left unattended, Devices must be password-protected or switched off, whilst data storage media must be placed in a secure storage facility.

5.3. Data processed electronically outside RISEBA's premises and which does not contain freely available public information must be encrypted at all stages of processing.

5.4. Users are prohibited from using email accounts belonging to other organisations for communication related to RISEBA's activities, as well as from forwarding any information related to RISEBA's activities to email accounts and/or cloud platforms belonging to other organisations.

5.5. Where there are no longer sufficient legitimate grounds for continuing data processing, in particular where the contractual relationship with the User has been terminated, the User must delete RISEBA data and destroy all copies. RISEBA may additionally inform the User as to which RISEBA data must be destroyed or returned to RISEBA.

5.6. Users are strictly prohibited from using public internet connections (e.g. in internet cafés, libraries, cafés, etc.) to access RISEBA data, except where the performance of contractual obligations takes place outside Latvia or where there is a critical and urgent need related to contractual obligations and the Resource Holder has given explicit consent to such activity. In all other cases, a mobile network must be used.

5.7. 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.

6. ACCESS MANAGEMENT

6.1. Any access rights granted to Users are assigned in accordance with contractual obligations and based on the 'need-to-know' principle. Access to any RISEBA system does not imply that the User is authorised to use all the information contained within such a system.

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

6.3. 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.

6.4. System security password requirements:

6.4.1. Users 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.

6.5. 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. This control applies regardless of whether the access attempt is made on a local data transmission network or a public data transmission network.

6.6. 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.

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

7.1. When performing contractual obligations on RISEBA's premises, the User must use RISEBA's equipment for data processing. Such equipment typically includes, but is not limited to, a desktop computer and/or a laptop with which the User can connect to RISEBA's servers and network. Where the use of RISEBA devices significantly hinders, delays or renders impossible the performance of contractual obligations in any specific case, as well as in cases where the User is working remotely, the User is permitted to use personal devices. When using personal devices, Users must comply with the requirements of clauses 5, 7.2 and 7.3 of this Provision.

7.2. Devices used by Users to fulfil their contractual obligations must meet the following requirements:

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

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

7.2.3. 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 the smartphone;
- The device must have the remote location tracking function enabled;
- Data and information must be stored in encrypted form.

7.2.4. 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;

7.2.5. 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.

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

7.4. If the User's device supports this feature, all RISEBA data must be stored separately from other data, in a folder with individual encryption and/or individual password protection. The User must delete RISEBA data from the device when its storage is no longer necessary for the performance of a specific work task or contractual obligation.

7.5. 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 file on the device containing RISEBA data; the User must also close any open windows or notification windows and immediately contact the Resource Holder to report the incident.

7.6. The Resource Holder and DPS must be informed immediately of the loss of a personal device on which RISEBA data was stored and processed.

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

8.1. Users are prohibited from using electronic data storage media 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 data classified as confidential or restricted access 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. It is prohibited to use electronic data storage devices that are damaged or do not function properly when working with RISEBA data.

8.5. No other person is permitted to access electronic data storage devices on which the User stores RISEBA data,

8.6. If data storage devices are handed over to other persons for use, the User handing over the device shall ensure that it does not contain RISEBA data and shall hand it over to another person for use only after deleting the data contained therein.

9. PROHIBITED ACTIVITIES

9.1. 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 User's contractual obligations or unrelated to RISEBA's operations.

9.2. The following activities are strictly prohibited:

(a) Infringement of 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) Any infringement of a data subject's rights by collecting and processing that data subject's personal data in an excessive manner and without a valid basis;
(d) Accessing data, a server or an account for purposes unrelated to the performance of RISEBA's activities or the fulfilment of the User's contractual obligations;
(e) Exporting software, technical information, encryption software or technology in breach of applicable international or national laws and provisions and/or RISEBA's instructions;
(f) Disclosing the User's access details to RISEBA systems and allowing other persons to use the personal 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 the User logging in to or accessing a server or account without specific authorisation, unless such obligations are the User's contractual obligations or access rights are granted to the User in connection with a specific RISEBA project;
(i) The use of any programme/script/command or the sending of any type of message with the aim of disrupting or disabling another user's session.

10. REPORTING AND HANDLING OF SECURITY BREACH INCIDENTS

10.1. The User must immediately report any data processing security incidents or incidents that may result in breaches of RISEBA's data processing security to both the Resource Holder and DPS.

10.2. The Resource Holder and DPS 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 staff and Management where necessary.

11. FINAL PROVISIONS

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

Document classification: RISEBA confidential information					
Title:	RISEBA Information Security Provision (Appendix No. 1)				
Responsible person:	Head of the IT Department	**Document approved by:**	Acting Rector of RISEBA		
		Document coordinated by	Data Protection Specialist		
Status:	In force	**Version:**	1.0	**Date:**	30 August 2022