Abbreviated security policy for electronic platforms of RSU information system

This document is a shortened version of RSU electronic platform security policy, which is intended to introduce RSU employees to the guidelines of RSU electronic platform security policy. Please also familiarise yourself with the full version of RSU electronic platform security policy.

RSU IS security management is based on the following principles[1]

- Legality. RSU information processing will be carried out only for the performance of the functions specified in laws and regulations and the information circulation process will comply with the security requirements specified in laws and regulations;
- Personal data protection. Access rights to personal data shall be limited to different scenarios depending on the status of a RSU employee and the duties to be performed;
- Only explicitly authenticated access to data by individuals. The user of any associated IS shall require unambiguous and secure authentication in order to be able to access its or other data. Any request for related IS must be clearly identified by the user who requested the data and, if necessary, in support of the request for data, otherwise such request will not be processed;
- Responsibility. A responsible person has been designated for each part of IS and information circulation procedure;
- Scalability. Financial contributions to information protection measures shall not exceed the possible direct and indirect financial losses in the event of security incidents. This principle does not apply to personal data protection;
- Monitorability. The IS should provide mechanisms to identify possible unjustified requests for information and provide for investigations into such cases. The analysis and evaluation of potentially unfounded and suspicious requests must take place in a sufficiently competent institution;
- Independence from external circumstances. Although it is not possible to establish a fully secure IS, provision should be made for a duplication of the main technical resources of is by deploying functionally equivalent technical resources in different geographically separated locations so that the impact of external circumstances (e.g. engineering network crash) does not halt the operation of IS.

[1] Security Policy for electronic platforms of RSU information system, paragraph 3

Confidentiality [2]

Depending on the range of persons authorised to receive information, there are three levels of confidentiality of information specified in is:

- Public (K1) information shall be freely accessible to all IS administrators and to any organization or person requesting such information. Dissemination of this information shall not negatively affect the operation of IS or related system controllers. The following information will be considered publicly available:
  - Documentation of use of IS.

- Internal use (confidential) (K2) information shall be protected from public access. The information is available to IS and associated system users with an appropriate level of rights. The information is not available to third parties and third party information systems without the appropriate permission. Unauthorised disclosure of the information to third parties may cause damage or inconvenience to the IS Controller, but the consequences are not critical. This level is granted to any information unless it is openly stated that it is public or secret.

- Classified (K3) information shall be protected from external and internal access. Access shall be allowed to users of IS and related systems who have authorisation to access specific information. If the information becomes known to a third party, there is a potential serious infringement of the data Subject's rights or significant loss to the IS Controller or the related system Controller.

Classified information includes:

- Any information about the identity and passwords of IS users;
- Any information on the personal data of the data subject.
- Registration of applications (registered with the data State Inspectorate);
- Registration of applicants (registered with the data State Inspectorate);
- Student registration (registered with the data State Inspectorate);
- Register of Library readers (registered with the data State Inspectorate).

The confidentiality rules specified in this section shall not apply to requests for information of law enforcement authorities received in accordance with the procedures specified in laws and regulations.

Value of the information resource [3]

The value of the information resource shall be characterised by the degrees of value, which may be as follows: high risk, medium risk or low risk.

- A high level of risk (R3) shall be granted to information if a security incident related to this information may endanger the continuation of the IS activity or result in a serious violation of the rights of third parties specified by law, or pose a direct threat to the life of the person.
  A high risk weight shall be granted to:

[2] Security Policy for electronic platforms of RSU information system, Paragraph 4.1.

[3] Security Policy for electronic platforms of RSU information system, paragraph 4.2.

  - Sensitive personal data;
  - IS service for software;
  - User identification information.

  The list shall be supplemented at the stages of the design and development of the system.

- A medium risk weight (R2) shall be assigned to information if a security incident related to that information is likely to seriously disrupt the activity or cause serious damage. A medium risk weight shall be assigned to:
  - System audit trail (insofar as it does not affect sensitive information);

  the list shall be supplemented in the design and development stages of the system.

- A low risk weight (R1) shall be granted to information the loss or disclosure of which to persons who are not authorised thereof does not cause serious damage or serious disruption to operation and does not constitute an infringement of the rights of third parties.
  A low risk weight shall be assigned to:
  - Information classified as publicly available;

IS users [4] - RSU employees or students or data subjects related to RSU. Rights and obligations of IS users: When receiving a username and password for access to IS, the IS User must confirm that they have read the IS security documentation by their signature. IS users, based on their access level or work tasks, may access the IS areas that they are eligible to use. The IS User must immediately notify the IS administrator (- s) of an IS security incident or/or malfunction.

General conditions for operating the information system applicable to RSU employees [5]

- Responsibility for ensuring information security has been clearly defined at all levels. The responsible employee shall be appointed for each information and technical resource. The staff Member responsible for ensuring the operation of this procedure shall be appointed for each information security procedure;
- The role and responsibilities of staff in ensuring security (in line with information security policy) are defined in job descriptions, employment contracts or other internal legislation;
- An agreement on confidentiality shall be concluded for the staff recruited on a permanent basis. The contract shall include liability provisions for the disclosure of non-public information. Breach of the Agreement may call on the is Controller the right to apply against professional activity insurance with a claim for recovery of losses;
- When signing the employment contract, the employee shall be introduced to the information determining the employee's responsibility for the security of the information;
- Security incidents shall be immediately reported to the is Controller's management in accordance with the established procedures;

[4] Security Policy for electronic platforms of RSU information system, paragraph 5

[5] Security Policy for electronic platforms of RSU information system, paragraph 6

- The IS users have a procedure governing the registration of security deficiencies and reporting to the Security Manager;
- Employees who violate or do not comply with information security policies or procedures shall be punished in accordance with external laws and regulations and RSU internal agenda;
- All IS users shall use unique identifiers assigned only to them in person so that each user's activities can be unequivocally identified and traceable;
- The creation and replacement of passwords shall be controlled automatically using the built-in features of IS;
- If necessary, digital signatures shall be used to verify the authenticity and integrity of the data in accordance with the existing procedures at RSU;

Electronic mail (e-mail) policy [6]

The policy of e-mail (e-mail) defines the main conditions regarding the authorised use of e-mail and compliance with security measures. This Policy includes procedures for receipt and sending of e-mails, which are carried out using technical resources of servers, workstations or mobile equipment at RSU's disposal.

1. Employee responsibilities

All employees of Riga Stradins University shall be obliged to activate user accounts in RSU e-mail system and to check their university e-mail accounts at least once a day, if the employee is not on holiday, business trip or any other justified absence from their workplace. If, for objective and reasonable reasons, the employee does not have the opportunity to check his or her university e-mail account at least once a day, the employee shall be obliged to check the aforementioned e-mail account as soon as such possibility is radusies.RS in the U e-mail system, the representatives of the technical and economic staff of the respective department indicated by the Head of RSU Department of Economic support or the Head of RSU Technical Service provision, as well as the representatives of the teaching ancillary staff, technical and economic staff of the respective academic department indicated by the Heads of RSU academic departments.

2. Property ownership

All e-mails and the system as a whole including all e-mails sent, and e-mail items used otherwise, as well as backup copies of e-mail items, shall be the property of RSU.

3. Monitoring

The authorised persons shall be responsible for monitoring the operation of the e-mail system in order to ensure the availability and continuity of the e-mail system. In order to ensure the security of the system, troubleshooting and, if necessary, to carry out certain investigative procedures, RSU shall have the right to monitor and check e-mail without prior notice.

[6] Security Policy for electronic platforms of RSU information system, paragraph 7

4. Responsibility

Employees shall be responsible for keeping e-mail access passwords and ensuring that their information is not disclosed to third parties. In cases where it is necessary to send restricted access information outside the organisation, the employee must obtain written evidence from the information Security Manager. In case of violation of e-mail policy, the employee may be subject to sanctions, for example: disciplinary proceedings or prohibition from using e-mail.

5. Ethical behaviour and responsible use

Staff should use e-mail only for work needs and to ensure the performance of organisational functions. The following are examples of responsible and irresponsible use of the e-mail system:

1. Ethical and appropriate use:

1.1. Communication by e-mail shall be carried out on the basis of job responsibilities and in accordance with the specified job functions;

1.2. By sending a reply to the e-mail received by the Service not later than within 24 hours (excluding holidays and public holidays) from the receipt of the letter. An exception to this paragraph shall be admissible if it is apparent from the content of the e-mail that no reply to it is required;

1.3. By filling in the field "Subject" ("Subject"), presenting the content of the e-mail precisely and briefly as possible;

1.4. Respecting their own and e-mail recipient's (recipients') time, by sending e-mails only when the sending is necessary;

1.5. In cases when e-mail is used to send information about the latest requirements of laws and regulations, procedures, processes or other internal documents;

1.6. In cases where notices have been sent to staff on certain activities - training, anniversaries, etc.;

1.7. Respecting the rights of all third party owners and licensors;

1.8. Ensuring that unwanted and old e-mails are deleted;

1.9. Respecting the same level of respect as when communicating verbal;

1.10. Checking grammar and correcting errors before sending an e-mail dispatches;

1.11. At the end of the e-mail containing at least the sender's name and surname, position and service telephone number;

1.12. In case of a business trip, holiday or other long-term absence, an automatic reply message shall be posted to the e-mail account, indicating:

- from which date the employee will not be available;
- a substitute (given name, surname, e-mail and telephone number) who is responsible for his/her competence during the employee's absence.

2. Unethical and inappropriate use:

2.1. Violating certain internal rules of procedure of the organisation (including any form of insulting, racism or other forms of discrimination);

2.2. By sending information containing inaccurate or defamatory information, including pornographic, racist and offensive material;

2.3. By sending personal information of a particular person or violating the rights of others to liberty by unauthorised use of information about that person at the disposal of the organisation;

2.4. By e-mail to carry out certain private activities for personal gain;

2.5. By sending entertaining and other information not related to the performance of official duties;

2.6. Including redundant elements in everyday business correspondence: colorful backgrounds for e-mails, unnecessary beauty elements, redundant decorations, etc.,

2.7. By attaching malicious software to e-mails;

2.8. By sending advertising or spam mail.

“Rules for the complications of RSU IS authorisation passwords”.[7]

Users shall be responsible for the safe storage of their passwords.

When an employee receives a new username and password, the password must be changed for the first time when logging on to the systems.

A combination of symbols that are difficult enough should be chosen as a password. The password must be at least 8 (eight) symbols long and not more than 16 (sixteen) symbols long.

The password must be changed at least every 192 days, and the new password must not be the same as 24 previous passwords.

After entering an incorrect password 5 times, a pair of username and password is excluded (*Lockout*) from the system for 30 minutes, the user shall immediately notify RSU IS administrator or the system manager about it.

The User shall be prohibited from disclosing any password assigned, as well as any other confidential information related to the use of RSU IS. The owner of the username and password used shall be responsible for each operation carried out in the computer network, databases, as well as other information systems.

If the User finds that someone else has exercised their rights, the User shall immediately notify RSU IS administrator or the system Manager thereof.

[7] Security Policy for electronic platforms of RSU information system, Annex 1

User passwords can only be stored in encrypted form on servers.