Consolidated version valid from 8 November 2024

APPROVED
by Order No. R-440 of 20 December 2021
of the Rector of Vilnius University
(wording of Order No. R-82 of 8 February 2024 of the Rector of Vilnius
University)

RULES FOR THE ADMINISTRATION OF USERS OF INFORMATION RESOURCES OF VILNIUS UNIVERSITY

CHAPTER I
GENERAL PROVISIONS

1. The Rules for the Administration of Users of Information Resources of Vilnius University (hereinafter the 'Rules') regulate the rights and obligations of the users of centrally managed or authenticated information resources of Vilnius University (hereinafter the 'University'), the user-rights administrators and other administrators and authorised persons, the administration principles of the access to the University's information resources used for the access to studies and internal administration purposes, and the procedure for secure provision of electronic information to users.

2. The University units responsible for public information systems, open access and other information resources of the University than those referred to in Item 1 shall be guided by these Rules or shall draw up user administration rules for the information resources under their management in accordance with these Rules and the specified legal acts.

3. The Rules have been prepared in accordance with the Description of General Security Requirements for Electronic Information approved by Resolution of the Government of the Republic of Lithuania No. 716 of 24 July 2013 "On the Approval of the Description of General Security Requirements for Electronic Information and the Description of Content Guidelines of Safety Documents" (hereinafter the 'Description of General Security Requirements for Electronic Information'), the Description of Organisational and Technical Cyber Security Requirements for Cyber Security Entities approved by Resolution of the Government of the Republic of Lithuania No. 818 of 13 August 2018 "On the Implementation of the Republic of Lithuania Law on Cyber Security" (hereinafter the 'Description of Organisational and Technical Cyber Security Requirements for Cyber Security Entities') as well as other legal acts and standards regulating the lawfulness of data processing, the activities of processors and the management of data security.

4. Terms used in these Rules:

4.1. **User of information resources** (hereinafter the 'user') – a person who does not perform the administrative functions regarding access to the University's information resources and who uses the University's information resources assigned to them on contractual or other legal grounds provided for in other documents of the University;

4.2. **Authorised person** – the head or designated employee of the University's core or its branch unit implementing the management of the University's information resource (hereinafter the 'unit implementing the management of the University's information resource'), authorised person responsible for data management, data protection officer, information security officer, or the employee's immediate superior who may instruct the user, user-rights administrator or other administrator to take additional actions with respect to the management of accounts and access rights;

4.3. **User-rights administrator** – an employee appointed by the head of the unit implementing the management of the University's information resource or an employee of the service provider referred to in Article 41 of the Republic of Lithuania Law on Management of State Information Resources who performs the management of access rights to the University's information

resource for the users, the users rights administration in accordance with the principles specified in the present Rules and performs other functions set out in these Rules;

4.4. **Account** – a set of personal data of a user necessary to identify the user and of registers of access rights to the University's information resources;

4.5. **University's information resources** – the totality of the information managed by the University in the performance of its functions, processed by information technology tools (system and network equipment, applications, modules, etc.) and the information systems and internal registers that process it;

4.6. **Management of the University's information resources** – setting the objectives for the creation, processing and development of the University's information resources, organising and supervising their processing and maintenance, organising and supervising the activities of the employees processing information, documents and/or their copies by means of information technologies.

4.7. Other terms used in the Rules shall be understood as defined in the Description of General Security Requirements for Electronic Information and other legal acts governing information resources as well as standards governing secure data processing.

5. The Rules shall be binding on all users and administrators of the University's information resources referred to in Item 1 of the Rules.

6. Access to the University's information resources shall be granted in accordance with the following principles:

6.1. access is granted only on legal grounds;

6.2. access is granted only after the user has been identified and authenticated;

6.3. access to modify (create, add or delete) data shall be granted only to those University's information resources which are necessary for the performance of the user's functions;

6.4. the functions of the user-rights administrator must be performed using a separate dedicated account, and, while using it, it is prohibited to perform user functions. Where the possibility to separate the roles of the user-rights administrators and the users is not implemented by means of an information resource, changes may only be made in agreement with the person authorised to enforce these Rules.

7. The rights to use the University's information resources are granted to the user only after acquaintance with the requirements of these Rules and the responsibility for non-compliance with them, and has committed to comply with them. Commitments shall be confirmed electronically, in a manner that provides evidence of familiarisation, at the time of the first login to the University's Identity Management System or the University's information resource. Where this option is not implemented in the University's information resource, consent must be confirmed in writing before the user is given the means of access.

8. Upon update of these Rules, all users shall repeatedly familiarise themselves therewith and confirm their commitment to abide thereby in the manner set out in Item 6 of these Rules.

9. Users are obliged to keep data and information secret. The obligation of secrecy shall apply even after ceasing the activities related to the processing of electronic information.

10. Users and user-rights administrators who violate the requirements of the Rules shall be liable in accordance with the procedures set out in the University's internal rules of procedure and the procedure set out in other legal acts regulating liability for violating information, cyber or electronic communications security and related violations.

CHAPTER II
THE POWERS, RIGHTS AND DUTIES OF USERS AND ADMINISTRATORS OF INFORMATION RESOURCES

11. The head of the unit implementing the management of the University's information resource shall have the right, insofar as is consistent with the unit's regulations, to:

11.1. process the information resources managed by their unit and provide access thereto;

11.2. if the responsibilities are not specified in the employee's job description, appoint user-rights administrators for information resources managed by their unit;

11.3. delegate part of the information resources processing functions managed by its unit to another unit, subject to its agreement.

12. Once a year, and no later than in 30 (thirty) working days after a structural change, the heads of the units implementing the management of the University's information resources shall organise a review of the access rights granted to users in selected units. The results of the review shall be recorded and, in the event of non-compliance with these Rules, adjustments to access rights to the information resource shall be made (in agreement with the head of the unit implementing the management of the University's information resource).

13. The users must:

13.1. enter only accurate data;

13.2. ensure the confidentiality and integrity of the data processed;

13.3. in the event of a change in the user's personal data indicated in the account, inform the employees of the unit to which the user has provided such personal data within 5 (five) working days of the change in such data, or within another period agreed upon with the employee referred to in this Item;

13.4. on receiving an instruction from an authorised person, rectify any errors detected and report on the actions taken immediately but no later than in 5 (five) working days, or provide the necessary information on the planned action if the instruction cannot be complied with immediately;

13.5. not interfere with the operation of the University's information resources and the accessibility of data;

13.6. not access centrally-managed information resources of the University using login names and passwords provided to other users;

13.7. not disclose or keep in plain sight the login names and passwords provided;

13.8. log out of their account when they have finished working with the University's information resources;

13.9. collect, process, transfer, upload, store, destroy, or otherwise use electronic information in information systems only employing a University-provided account for work purposes;

13.10. after finishing work, ensure that electronic information is not accessible to other persons, activate a password-protected screen saver when leaving their workstation;

13.11. destroy electronic information at the instruction of an authorised person;

13.12. comply with the requirements of legal acts on the protection of personal data and cyber and information security;

13.13. immediately notify the Helpdesk of the Information Technology Support Division of the University's Information Technology Service Center (hereinafter the 'Helpdesk') or the administrator of the computerised workstation of their unit about any malfunctions of the University's information resource, unusual functioning, actual or potential violations of the requirements of the security of electronic information, or improper actions of other users.

14. The electronic information of the University's information resources is processed by user-rights administrators and other administrators – system administrators, software administrators, local network and computerised workstations' administrators.

15. System administrators:

15.1. process the rights of administrators;

15.2. process user rights and account credentials on the instruction of authorised persons;

15.3. process records of users' activities on the instruction of authorised persons;

15.4. back up and delete electronic information in accordance with internal procedures and time limits.

16. Software administrators:

16.1. process records of users' activities;

16.2. destroy electronic information on the instruction of authorised persons;

16.3. review user rights;

16.4. process descriptions of user rights groups (roles) on the instruction of authorised persons;

16.5. prepare reports on user-rights administration on the instruction of authorised persons.

17. User-rights administrators:

17.1. grant, modify, suspend, terminate, and otherwise process user rights;

17.2. process the identification data of user accounts if it is not processed automatically;

17.3. destroy electronic information on the instruction of authorised persons;

17.4. prepare reports on users-rights administration on the instructions of authorised persons;

17.5. review user rights.

18. Local network and computerised workstations administrators process records of the system software, network, and related user activities of the computerised workstation.

19. The administrators referred to in Item 14 of the Rules shall have the right to:

19.1. with prior notification to the user, at any time block the user's access to any of the University's information resources if the user violates the requirements of these Rules; prior notice is not necessary when it is essential to act promptly to block a user's access due to a serious threat to data security;

19.2. require users to adjust data or provide additional information should this be necessary for the purposes of processing the University's information resources.

20. The administrators referred to in Item 14 of the Rules, following the instructions of their immediate superiors, heads of units, and information resources security officers, shall be obliged to provide information to the authorised State institutions about users when it is necessary to provide such information in accordance with the requirements of the legal acts of the Republic of Lithuania.

CHAPTER III
THE PROCEDURE FOR CONTROLLING THE SECURE PROVISION OF ELECTRONIC INFORMATION TO USERS OF INFORMATION RESOURCES

21. The procedure for registering and suspending user access:

21.1. all members of the University community who wish to become users of the University's information resources shall register within the University's Identity Management System;

21.2. login data of users of information resources not connected to the University's Identity Management System shall be provided to users in accordance with the procedure established by the units implementing the University's information resources management;

21.3. the information required for user registration of members of the University community who wish to become users is automatically obtained from the University's Human Resources Information System and the University Study Information System;

21.4. a new member of the University community who wishes to become a user shall provide a unique first login code during registration. The unique first login code shall be given to a person who concludes an employment, study or other contract/agreement or submits another document on the basis of which the person becomes a member of the University community. The unique first login code shall be provided by the persons responsible for the conclusion of the contracts/agreements and/or other documents referred to in this Item;

21.5. other persons than those referred to in Items 21.1–21.4 of the Rules who wish to become users (hereinafter the 'other users') and obtain access to the University's information resources which they need in order to ensure the fulfilment of other agreements concluded with the University (e.g. service provision) or on other legal grounds shall be provided with a login name and temporary password that they have to change during their first login; the login name and temporary password for the persons detailed in this Item shall be provided by the Helpdesk responsible for the creation of the account or the unit implementing the management of the University's information resource;

21.6. the login data shall be provided no later than in 2 (two) working days after the decision to grant access rights;

21.7. the suspension (restriction) of users' rights occurs after the expiry of the time limit for which the access right was granted, or after the contract or other legal basis ceases to exist, or at the direction of authorised persons, following the procedure for reviewing, modifying and terminating access rights as provided for in these Rules.

22. The procedure for granting users access rights to the University's information resources:

22.1. upon granting the access, the minimum set of the University's information resources required for the performance of the functions specified in the contract, job description or other document governing the user's status is detailed;

22.2. before the user is granted with access to additional University's information resources, the user must have submitted a request whose content is specified in Item 24 of the Rules, prepared by means of the University's document management system, or a request in the form specified by the unit implementing the management of the information resource;

22.3. requests shall be submitted by the user or by the responsible employee of the unit implementing the system management or maintenance functions (hereinafter the 'responsible person') if the user is unable to submit the request themselves for objective reasons;

22.4. the request must be coordinated with the head of the unit concerned and the head of the unit implementing the management or processing of the University's information resource, where such is appointed in accordance with Item 11.3 of the Rules, or their appointed person;

22.5. the request must be submitted at least 2 (two) working days before the additional requested access rights are granted;

22.6. Upon receipt of a request, the unit implementing the management of the information resource, or the Helpdesk in the case of centrally managed information resources, shall verify that the request has been coordinated with the persons referred to in Item 22.4 and that all the intended data controllers have been included; if any adjustments are necessary, the request shall be returned to the originator;

22.7. the request shall be registered and transferred to the user-rights administrator or system administrator of the University's information resource specified in the request for implementation no later than the next working day;

22.8. when additional rights of access to the University's information resources are requested to be provided on a temporary basis, the maximum duration of the temporary grant may be up to 1 (one) year;

22.9. when a software licence is granted, the granting of the licence shall be recorded by the administrator of the computerised workstation in accordance with the procedure laid down by the University's legal acts;

22.10. upon having granted the access rights specified in the request or having completed the steps required to obtain access or a licence, the request-submitting user and/or the responsible person shall be notified. If necessary, other persons may be informed.

23. To administrators, authorised persons responsible for data management and security, the rights are conferred according to the procedure established in Item 22 of the Rules; however, in such case the request shall be made by the head of the unit where the persons concerned work or by an employee of the unit appointed thereby, and the decision on the granting of rights shall be taken by the head of the unit implementing the management of the University's information resource, or by an employee of the unit appointed by them.

24. The request for registration of access to information resources and for the granting, modification, and removal of rights shall contain the following information:

24.1. the legal basis for granting access:

24.1.1. if the basis is a concluded contract, the registration number and date of the contract is indicated. If the contract is yet to be concluded, it is a must to indicate the date on which it will be concluded or enter into force;

24.1.2. if access rights are granted on other legal grounds, such other legal ground shall be indicated;

24.2. the name of the University's information resource, the user's unit or the unit responsible for the user, the user's full name, date of birth (if the user is not a member of the University's community), and the time limit for which access rights are required (if the legal basis for granting access is an open-ended contract, enter 'open-ended');

24.3. the requested access rights to the University's information resource (e.g. the name of the role, the scope of the rights in terms of units, projects, types of funds).

25. The procedure for reviewing and modifying access to the University's information resources:

25.1. when a user is transferred to another position within the University or when the user's functions change, the user, their immediate superior or an employee appointed by the head of their unit shall, via the University document management system, prepare a request (whose content is specified in Item 24 of the Rules) for reviewing the rights of access indicating a change in the user's position and/or work functions and/or the need for specific information resources of the University, and submit it to the unit implementing the management of the information resource or the Helpdesk;

25.2. the user-rights administrator shall review user rights upon request within a maximum of 5 (five) days, except in the case of incidents, where the review shall be carried out immediately, on the same or the next working day.

26. Procedures and cases of suspension and/or termination of the user and/or administrator's access to the University's information resources:

26.1. the user and/or administrator's access to the University's information resources may be suspended and/or terminated:

26.1.1. in the event of objection to or refusal of the processing of personal data relating to a user account;

26.1.2. in the event of the user's job position and functions having changed;

26.1.3. in the event of the user having been removed from office;

26.1.4. in the event of finding a breach of employment duties or other contract;

26.1.5. in the event of suspecting or detecting illegal use of the University's information resources or user data;

26.1.6. in the event of receiving a notice by the authorised person on the termination of a particular user's access to specific information resources;

26.1.7. in the event of cases specified in the procedure for the information systems incident management;

26.1.8. in the event of the administrator having not logged into the system for more than 3 (three) months and the user having not logged into the system for more than 6 (six) months;

26.1.9. when an investigation into the activities of an administrator or user is performed;

26.1.10. in the event of the administrator or user refusing to execute instructions and orders of authorised persons;

26.2. the user and/or administrator's access to the information resources processed is suspended and/or terminated by submitting a request whose content is specified in Item 24 of the Rules or immediately upon the instruction of an authorised person.

26.3. The user-rights administrator shall suspend and/or terminate user rights upon request within a maximum of 5 (five) days, except in the case of incidents, where the suspension shall be effected immediately, on the same or the next working day.

26.4. In the event of suspension and/or termination of access, the user account registration data must be stored electronically for a minimum period of 6 (six) months (except as provided for in other legal acts), after which it may be archived.

27. The procedure for terminating access to the University's information resources:

27.1. users who are members of the University community shall have their additional access rights revoked at the end of their contractual relationship with the University or the time limit specified in the request, but they shall retain a special set of rights and access to the University's information resources (e.g. email) for a period of 14 (fourteen) days, which shall only provide access

to the user's own personal data. Upon expiry of the period of 14 (fourteen) days referred to in this Item, access shall be automatically terminated;

27.2. access rights for other users are automatically terminated upon expiry of the time limit specified in a request submitted according to the procedure specified in Item 22.2 of the Rules or earlier, at the end of the contractual relationship with the University, or the termination or expiry of other legal basis without a transitional period;

27.3. at the reasoned request of the user or the responsible person (e.g. for the full implementation of contractual obligations or other circumstances provided for in the Labour Code or collective agreement), and upon the agreement of the responsible person at the unit exercising the functions of information resources controller or processor, the minimum access period may be extended up to a maximum of 1 (one) year.

28. Means to identify users:

28.1. in order to identify users when accessing the University's information resource, a username and password for logging in to the University's information resources must be provided as well as one of the multi-factor access control systems indicated in Item 28(4) of the Rules must be used (when enabled);

Amendments to the Item:

by Order of the Rector of Vilnius University No. R-462 of 8 November 2024.

28.2. login data shall only be provided to subjects whose identity is verified in accordance with the procedure set out in the Description of the Procedure for the Processing of Personal Data at Vilnius University approved by Order of the Rector of Vilnius University No. R-316 of 25 May 2018 "On the Approval of the Description of the Procedure for the Processing of Personal Data at Vilnius University" (wording of Order of the Rector of Vilnius University No. R-391 of 25 September 2020);

28.3. information on how to log in to the University's information resources is provided during the session of introduction to information resources;

28.4. administrators and users must choose and use one of the multi-factor access control systems:

28.4.1. software access code generators (e.g. on mobile phones);

28.4.2. phone call or informing via an SMS message.

Amendments to the Item:

by Order of the Rector of Vilnius University No. R-462 of 8 November 2024.

28.5. where technical possibilities permit, administrators and users processing personal data or other confidential information may be enabled to use other multi-factor access control systems:

28.5.1. electronic signature;

28.5.2. nominal certificate;

28.5.3. access key;

28.5.4. biometric measure (e.g. a fingerprint).

Amendments to the Item:

by Order of the Rector of Vilnius University No. R-462 of 8 November 2024.

28.6. users wishing to use multi-factor access control systems detailed in Item 28(5) of the Rules in order to access the University's information resources must submit a request to the Helpdesk which shall make a decision on the submitted request, taking into account the job position and functions performed by that employee.

Supplemented with the Item:

by Order of the Rector of Vilnius University No. R-462 of 8 November 2024.

29. Requirements for the creation, validity, and change of user passwords:

29.1. the first time a user logs into the University's Identity Management System, they must change the one-off password if such has been provided;

29.2. if the user forgets the password, access to the University's information resources will be granted:

29.2.1. by providing the data required to restore access in the self-service of the University's Identity Management System as specified in the University's Identity Management System at the time of the first login or by adjusting the data at the time of the next login;

29.2.2. by the user submitting request to the unit or the Helpdesk;

29.3. the user must keep the password secret and not disclose it to third parties, and must change it immediately if they suspect that third parties have learned the password;

29.4. the password must be composed of letters of the Latin alphabet, numeric characters and special characters as provided in the ASCII encoding;

29.5. the password must contain at least one uppercase and one lowercase letter, a numeric character, and a special character;

29.6. the password may contain only two identical consecutive characters;

29.7. diacritical marks (including the letters ą, č, ę, ė, į, š, ų, ū, ž of the Lithuanian alphabet) may not be used in the password;

29.8. the following special characters are not recommended for a password: /, :, !, \, %, |, $;

29.9. passwords must not contain personal information (e.g. date of birth, names of family members, etc.);

29.10. passwords must not contain popular place names, personal names, or other commonly used words in Lithuanian or English;

29.11. unless otherwise specified in separately approved documents implementing the University's or the State's information resources security policy:

29.11.1. the password for the user account must be changed no less frequently than every 120 (one hundred and twenty) days;

29.11.2. the password for the user account must be at least 8 (eight) characters in length;

29.11.3. when the password is about to expire, the user must be given a 10 (ten) days notice and a 5 (five) days notice to change the password;

29.11.4. for the University's information resources where multi-factor authentication has been implemented, the master password may be valid for one year, but the additional device code must be generated uniquely for each login session;

29.12. users who do not administer special categories of personal data and other confidential information, when this is implemented in an information resource, are allowed to enable the option of remembering the authorised device and not be required to enter an additional code. If the user has not logged in to the University's information resource for more than 30 (thirty) days, they shall be asked to additionally authenticate with the password (and an additional code if the user has opted for multi-factor authentication);

29.13. the password to be changed must not be identical to at least 6 (six) previous passwords;

29.14. it should be prohibited to change the password a second time in less than 24 (twenty four) hours, unless the password became known to another person. In this case, the Helpdesk may grant the right to change the password once again.

30. Additional password processing requirements for users and administrators processing confidential information or multi-unit personal data:

30.1. the password must contain at least 12 (twelve) characters;

30.2. the password must be changed at least every 3 (three) months, unless multi-factor authentication is used for login. In this case, the master password may be valid for up to 180 (one hundred and eighty) days.

30.3. The time limit set out in Item 29.11 of these Rules shall be valid for systems that do not process confidential and/or personal data and for specialised technological devices specified in Item 32 of these Rules.

31. Information technology components that authenticate the identity of the user must prohibit the automatic storage of passwords, except for specialised password managers (e.g. applications implementing two-factor password protection) that provide an adequate level of security.

32. Requirements specified in Items 28–31 of the Rules for specialised technological information resources (information resource infrastructure required for specific functions, technical equipment such as medical, measurement equipment or that required for experiments, specialised classroom and laboratory equipment, meteorological or metrological stations, specialised data collection devices, controllers and SCADA devices, meters, data encryption devices with encryption

software installed by the manufacturer, etc. which are supplied by the manufacturer with the software but which, by their purpose and nature, cannot be hosted in data centre premises or are intended for specific functions of research or technological processes) shall be applicable insofar as their technical feasibility permits but shall not be subject to requirements weaker than those laid down in Annex 1 to the Description of Organisational and Technical Cyber Security Requirements for Cyber Security Entities.

33. The following account access recovery measures shall be implemented in the University's information resources (where technically feasible):

33.1. sending a confirmation code to the mobile phone number of an EU operator indicated and verified in the user's account;

33.2. sending a link to the access recovery form to the backup personal email address specified in the user's account;

33.3. on the self-service page of the University's Identity Management System, using a circumstance or key phrase of at least 12 characters that is known only to the user and was entered at the time of account creation;

33.4. calling the Helpdesk at +370 (5) 236 6200 from the backup account recovery phone number specified in the user's account, confirming the secret phrase entered when creating the account and two personal details (personal identification number, employee's tabular or student identity card number, full name of the emergency contact person). In order to ensure that the account cannot be compromised in this way, the employees of the Helpdesk shall have the right to ask additional identification questions other than those provided for in this Item;

33.5. after changing the password, the user shall receive a text message about the login attempt at the email and mobile phone number provided in the user's account.

34. A maximum number of attempts by the user to enter the correct password, phrase or select the correct image (reCAPTCHA) (up to a maximum of five (5) attempts within 15 (fifteen) minutes from the same IP address if the information resource supports such functionality) shall be set. If the password is entered incorrectly in succession or the image is selected incorrectly for the number of times set, the user's account access from such IP address shall be locked and the user shall not be allowed to connect for at least 15 (fifteen) minutes. Where it is technically feasible, a text message on the attempted login using the primary email and mobile phone numbers provided in the user's account shall be sent to the selected account recovery (backup) contact of the user.

35. Administrators and users who process other persons' data or other confidential information remotely must use Vilnius University's virtual private network or other secure tunnel to connect to information resources, i.e. connection to information resources shall be possible only via an encrypted channel. The communication shall be encrypted using a key of at least 256 bits.

36. Connections and/or attempts to connect to the University's information resources over IP networks are automatically logged in action logs. The registration data shall include the date, time and duration (if any) of the login and/or attempted login, the username of the user who logged in or attempted to log in and the IP address of the computer from which the login or attempted login took place, the functions accessed, the list of actions performed on the personal data (input, review, modification, destroying, and other data processing actions). These records shall be retained for at least 6 (six) months.