Rīga Stradiņš University Dataverse Maintenance Plan

1. General provisions and purpose

1.1. The purpose of this document is to determine the principles of maintenance, ensuring of operation and continuity of the RSU Dataverse (hereinafter – the Repository) institutional research data repository of Rīga Stradiņš University (hereinafter – RSU).

1.2. The maintenance plan shall be provided by the Repository:
- long-term availability;
- the integrity and security of the data deposited;
- compliance with internationally recognised repository standards.

1.3. The maintenance of the repository is implemented in accordance with the internal regulatory enactments of RSU, including IT-10 is an internal regulatory document of Rīga Stradiņš University, which defines the basic requirements for the security, maintenance and continuity of information systems in the RSU information technology environment.

2. Monitoring the maintenance of the repository

2.1. RSU Data Curators in cooperation with the RSU Information Technology Department (IT Department) are responsible for the general maintenance strategy and coordination of the Repository' s activities.

2.2. The IT Department shall ensure the technical maintenance of the Repository:
- restoring the system and ensuring its uptime;
- the creation of backup copies and the possibility of restoration;
- the safety and accessibility of infrastructure;
- incident management in accordance with RSU's internal procedures.

2.3. Maintenance activities are documented in RSU internal information systems in accordance with IT-10 requirements.

3. Software maintenance

3.1. The operation of the repository is based on open source [Dataverse software](), which RSU maintains and updates in accordance with the principles of good practice.

3.2. Software updates are made regularly, paying special attention to:
- security improvements;
- the stability of the system;
- interoperability with the RSU information systems environment.

3.3. Before implementing changes in the Repository's operating environment, they are tested in the testing environment in accordance with the procedures specified by RSU.

4. System availability and operability

4.1. The Repository is maintained in an infrastructure managed by RSU, ensuring accessibility to Users 24 hours a day, 7 days a week, except for planned maintenance works.

4.2. Planned maintenance works are carried out as necessary, Users are informed about them in advance, as far as possible.

4.3. The operation of the system is monitored using automated monitoring solutions that:
- continuously monitor the availability and upability of the system;
- automatically generates malfunction notifications.

4.4. In case of system malfunctions, RSU IT incident management processes are applied, ensuring:
- recording the incident immediately;
- the initiation of a reaction within no later than 1 working hour in the event of a critical disturbance.

4.5. The *Recovery Time Objective (RTO)* is up to 12 hours, depending on the nature of the incident.

5. Data security and backups

5.1. All data stored in the Repository are stored in the infrastructure managed by the RSU IT Department, to which physical and logical access is provided only to authorised persons.

5.2. Data backup copies are created in accordance with the RSU backup copying procedure by applying the GFS (Grandfather–Father–Son) principle:

- daily backup copies – 1 time in 24 hours, storage period 5 days;
- weekly backups – 1 time per week, storage period 1 month;
- monthly backup copies – 1 time per month, storage period 6 months.

5.3. Backup copies are stored in encrypted form and in a physically segregated environment to reduce the risk of data loss in emergency situations.

6. System documentation

6.1. All significant changes to the Repository configuration are documented in the documentation and version management environment specified by RSU.

6.2. The procedures for maintaining and restoring the system are described in the internal documentation of the RSU IT department.

6.3. The documentation shall be:

- reviewed after each significant system change;
- updated at least once a year.

6.4. In addition to the technical documentation, the RSU Dataverse Repository has developed the Terms of Use and the User Manual, which determine the procedure for using the Repository, the rights and obligations of Users, as well as practical guidelines for working with the system.

6.5. The Terms of Use and the User Manual are interrelated with this maintenance plan and are maintained in an up-to-date version, ensuring the coherence of the Repository's management, technical maintenance and User activities.

7. Controls and audits

7.1. The RSU IT Department performs a periodic review of the technical activities of the Repository at least once a quarter, evaluating:

- the availability of the system;
- security events;
- the execution of backup copies.

7.2. Access and activity logs are maintained and stored for not less than 6 months, in accordance with RSU's internal security requirements.

7.3. The operation of the repository is regularly reviewed in cooperation with the Data Curators in order to identify:

- the necessary technical improvements;
- opportunities for improving data quality and governance.

7.4. The evaluation of the operation of the repository also takes into account compliance with the Terms of Use and the User Manual, including:

- Compliance of user actions with the established roles and access rights;
- compliance with the procedures for the insertion, management and use of data;
- cooperation with Data Curators in ensuring data quality.

8. Continuity plan

8.1. The continuity of operation of the RSU Dataverse Repository is ensured by using the backup of critical system components at both the infrastructure and data level, ensuring the primary and backup operating environments.

8.2. In case of infrastructure disruption or system failure, the restoration of data stored in the Repository from automated backups is possible within 6-12 hours, depending on the type of incident and the affected part of the system.

8.3. The RSU Information Technology Department has developed and maintains a Disaster Recovery Plan (DRP), which determines the procedures for restoring the operation of the Repository in emergency situations.

8.4. The DRP shall include:
- system recovery time objective (RTO) not exceeding 12 hours;
- the permissible data loss limit (RPO – Recovery Point Objective), which does not exceed 24 hours;
- the sequence of activities, responsible persons and the procedures for cooperation between the rsu departments involved.

8.5. The DRP is regularly reviewed and tested at least once a year, as well as after significant changes in the infrastructure or software of the Repository.

8.6. DRP documentation is stored in a secure documentation environment of the RSU IT Department and is available to Data Curators to ensure the continuity of the Repository's operation.

9.Provision of funding for the repository

9.1. The maintenance, development and operation of the Dataverse repository of Rīga Stradiņš University shall be financed from the basic budget of Rīga Stradiņš University.

9.2. Funding from the RSU basic budget is provided by the Repository:
- long-term business continuity;
- maintenance of technical infrastructure;
- software update;
- ensuring data security and backup copies;
- the implementation of support functions (involvement of data curators and the IT department).

9.3. The financing of the Repository does not depend on the availability of individual projects or short-term external sources of financing, thus ensuring institutionally sound and sustainable operation of the Repository.

10. Review

10.1. The RSU Dataverse Repository maintenance plan is reviewed at least once a year, as well as after significant changes in the Repository's software, infrastructure or management processes.

10.2. The review of the maintenance plan shall be coordinated by the Department of Science in cooperation with the Data Curators and the RSU Department of Information Technology (IT Department).

10.3. Within the framework of the review, the following shall be assessed:
- Technical operation and availability of the repository;
- the adequacy of data security and continuity measures;
- up-to-date documentation, including the Terms of Use and User Manual;
- compliance with RSU's internal regulatory enactments and applicable international standards.

10.4. After the review, the necessary amendments are documented and implemented in accordance with the procedures specified by RSU.