

Subject area: Archive and registry and Security and information security

Document type: Objectives/strategy

Decision-maker: Vice-Chancellor

Organisational unit: Vice-Chancellor's Office/Legal
Affairs and Documentation Unit

Reference: Renata Arovelius

Decision date: 24/5/2016

Effective as of: 24/5/2016

Valid until: further notice

To be updated by: 1/1/2018

Document(s) repealed: -

Annex to: Decision, SLU ID: SLU.ua.2016.2.1.2-1990-2

Strategy for preserving electronic records

This governing document is SLU's strategy for preserving the university's electronic records in accordance with RA-FS 2009:1, Chapter 3, Section 1–5.

The digital records at SLU comprise all operations and can be found in central administrative systems such as Ladok, Agresso, etc.; data management systems for research and EMA; virtual learning environments and other support systems within the university administration; it can also be information in varying digital formats for image, film or sound.

The preservation strategy assumes that there is an e-archive, i.e. a system for preservation and/or an operational system with built-in e-archive functionality.

Strategy objectives

- SLU has a good structure for public access and enables the public and researchers to easily access public records, including data from research and EMA. This means that:
 1. Electronic records are managed and documented, which means that registration is done continuously according to SLU's classification scheme and archival description.
 2. Employees affected by record management are familiar with the applicable regulations, including those on preservation and security requirements.
 3. The university fulfils the requirements for processing and managing personal data.
- SLU facilitates easy access to data affected by regulations or procedures for open access, open science and open data.

- SLU has efficient and quality-assured processes for documenting and managing electronic records. This means that:
 1. Preservation actions are integrated in the operation's work processes.
 2. Preservation planning and follow-up is an integrated part of internal governance, control and risk analysis work.
 3. Electronic records are searchable, authentic, reliable and reusable.
 4. SLU follows policies and guidelines for information security in accordance with decision SLU ID: SLU.ua.2015.2.10-2118.

Responsibility and roles

Main responsibilities

- The head of university administration is responsible for ensuring that there is a suitable and sustainable infrastructure for preservation of and access to electronic records, including research and EMA data.
- The Legal Affairs and Documentation Unit is responsible for establishing regulations and procedures for preservation and access to electronic information in accordance with the Public Access to Information and Secrecy Act as well as for providing support when preservation plans are drawn up.
- The Division of IT is responsible for cataloguing all systems, system documentation and coordinating the strategy with SLU's IT policy.

Persons responsible for archives

- Formal responsibility for an archive lies with the head of department/equivalent. The operative responsibility may be delegated to an administrative manager or a person with a registry and archiving role.
- Persons responsible for archives coordinate the preservation of electronic records in operational systems in accordance with an established preservation plan, and make sure that procedures are followed.
- Persons responsible for archives ensure that no system or digital storage space is abolished before long-term preservation has been secured.

System owner

- A system owner is responsible for ensuring that there is a preservation plan for operational systems. The operative responsibility may be delegated to a system manager/equivalent.
- Developing a preservation plan must be done in conjunction with the Legal Affairs and Documentation Unit.
- If there is no system manager or person responsible for a digital storage space, the person responsible for archives establishes a preservation plan.

SLU employees

- All employees are responsible for ensuring that public records, regardless of format, are managed in accordance with current preservation regulations.

Preservation plan and records

- A template for a system inventory and a preservation plan must be available on the web.
- The plan must contain information on:
 - Which information can be found in the system (type of data, data organisation, operational process in which the data has its provenance, system description);
 - Metadata;
 - Data format, file names;
 - Restrictions on availability and reuse, e.g. confidentiality and copyright;
 - Appraisal and disposal regulations;
 - Migration actions;
 - Frequency of transfers to long-term preservation;
 - Schedule and measures if a system is to be abolished;
- The current preservation plan must always be registered in a records management system according to SLU's classification scheme and archival description.

Technical requirements and format

Technical requirements

- When producing electronic records, SLU must follow the technical demands specified in RA-FS 2009:2 (the Swedish National Archive's regulations and advice on technical requirements for electronic records).
- If that is not possible, the records must fulfil the technical requirements at the latest when they are transferred to long-term preservation. Transfers must occur as soon as possible.
- In such cases, the minimal requirement is to ensure that the records can be exported from an operational system and that they are preserved in approved formats.

Format

- SLU must follow the Swedish National Archive's recommendations when choosing format.
- SLU must, to the greatest possible extent, select open formats irrespective of the producer.

- A template for agreements with information producers in accordance with ISO 14721:2012, OAIS (Open Archival Information System), together with a list of recommended formats, must be available at the latest when the e-archive is deployed.

E-archives

- SLU must provide a customised and sustainable system for long-term preservation of electronic records.
- Operational systems that fulfil the e-archive functionality requirements should act as intermediate archives.
- The head of university administration is responsible for ensuring that there is a sustainable e-archive.
- The Legal Affairs and Documentation Unit is responsible for ensuring the quality of records preserved in the e-archive and for planning long-term preservation in the e-archive.

Follow-up

- SLU's strategy for preservation must regularly be reviewed and revised as technical changes occur.
- System preservation plans containing public records must be reviewed and revised annually. The revision work must be documented and reported back to the head of university administration.

Appendix: Definitions

Preservation plan	Plan for preserving, appraising and disposing of electronic records in an operational system or digital storage space.
E-archive	System for preservation and/or an operational system with e-archive functionality. Contains functions for transferring records, filing, storage, appraisal and disposal, availability/distribution, retrieval and administration.
Electronic records	Material recorded for automatic data processing in accordance with Chapter 2, Section 3 of the Freedom of the Press Act (1949:105).
Appraisal and disposal	The destruction of public records or data in public records. A change of media involves appraisal and disposal if it causes important data loss, loss of possible compilations, loss of search possibilities or if the possibility to assess the authenticity of the record is lost.
Records management	Includes all documents that govern SLU's archiving, including 1. Content description 2. Archival inventory 3. Classification scheme SLU KS 2013:1-1, including the description of all operational processes and record types 4. Current documentation management plans.
Classification scheme and archival description	System for managing SLU's operational information. As of January 2013: Public 360°.
ISO 14721:2012 OAIS	General model for an Open Archival Information System. OAIS is an e-archive consisting of a system and persons responsible for long-term preservation and who have access to electronic records over time.
Intermediate archive	Here: operational system with built-in e-archive functionality.
Metadata	Descriptive and preservation metadata that document content and context and secure access to data over time.
Open Access	“Open Access refers to online, free of cost access to peer reviewed scientific content with limited copyright and licensing restrictions.” https://www.fosteropenscience.eu/

Open Data	<p>“Open Data are online, free of cost, accessible data that can be used, reused and distributed provided that the data source is attributed.”</p> <p>https://www.fosteropenscience.eu/</p>
Open Science	<p>“Open science is the movement to make scientific research, data and dissemination accessible to all levels of an inquiring society.”</p> <p>https://www.fosteropenscience.eu/</p>
Security classification	<p>In accordance with SS-ISO/IEC 27001:2006, Information technology – Security techniques – Information security management systems (LIS). SLU applies security classification on the basis of the impact for the whole university in accordance with the Swedish Civil Contingencies Agency (MSB). Security classifications are stated in numbers, e.g. 0, 1, 2, etc.</p>
Availability/access	<p>“Right, opportunity, or means of finding, using, or approaching DOCUMENTS and/or INFORMATION”</p> <p>http://www.narc.fi/nat/</p> <p>“The function that provides archival information and adjoining services to those who take part of the archival information.”</p> <p>The National Swedish Archive – eARD – glossary.</p>