Terms of use for ERDA/SIF

These terms of use for ERDA and SIF ("**the Systems**") set out the terms and conditions applying for the use of the Systems ("**the Terms**"). The Terms apply to all users of the Systems, as defined below.

The Systems are subject to Aarhus University's information security policy. All updates to this policy are therefore inherited and applied to this document, even if the updates are not reflected directly in the document.

Purpose of the Systems

The Systems are Aarhus University's campus solutions for storing research data. ERDA is the solution for storing and sharing general research data, while the SIF solution provides an extra layer of security when processing sensitive research data, including personal data, confidential information from a third party, IP-sensitive information, URIS data, data subject to export controls, and data that must be protected against unauthorised access for other reasons.

Scope and target group

The Systems are intended for research data only and may not be used for processing other types of data, e.g. data handled for administrative purposes. The Systems must therefore be used only by academic staff, their external collaborators – subject to their acceptance of the Terms – and technical/administrative staff in connection with research-related activities in specific research projects ("**the User"/"Users"**).

The user's role and responsibilities

The use of the Systems is associated with a high level of security and clear expectations for correct user conduct. As a User, you undertake to use the Systems in accordance with all applicable legislation, Aarhus University's internal rules, and these Terms.

Conditions for access and account creation

Internal Users

Employees at Aarhus University (including researchers, PhD students, research assistants and student assistants) can access the Systems by virtue of their employment, provided that they have completed the mandatory user course and are affiliated with a relevant research project. They must also be registered as Users of the Systems.

The research coordinator (PI, principal investigator) is responsible for assigning access and ensuring that all internal Users:

- have a legitimate need for access to the project in question,
- are familiar with and comply with all applicable rules for data security and proper use.

External Users

External project partners can be granted access to the Systems as Users provided that:

- a concrete and active research collaboration exists between Aarhus University and their employer institution, or between Aarhus University and individuals who make use of the Systems,
- the User accepts these Terms of Use of the Systems,
- the User is affiliated with one or several project folders in a specific project, and
- access has been approved by a contact employed at Aarhus University, who is responsible for the project.

External Users may only access data to the extent necessary for their participation in the project, and their access must be continuously reassessed by the research coordinator.

Pre-access requirements

Access requires that the User:

- has completed the mandatory user course,
- accepts the applicable Terms of Use,
- and, to the relevant extent, is familiar with and complies with Aarhus University's data protection, information security, and research data management guidelines.

System access is personal and may not be shared with others. Use of joint accounts is not permitted, and Users may only use their access personally.

Purpose of use

The systems must only be used for storage and management of research data.

- **ERDA** must be used for general research data.
- **SIF** must be used when increased security is needed, for example when processing data that:
    - contain personal data (including pseudonymised personal data),
    - form the basis for patenting the research results,
    - contain confidential or IP-protected material from a third party,
    - are subject to export controls or dual-use regulation,
    - are strategically important or sensitive (e.g. URIS data),
    - or for any other reason should be protected from unauthorised access or sharing.

It is not permitted to use the Systems for administrative purposes or for storing data types other than research data.

Prohibitions and unacceptable use

In order to maintain the necessary System security and integrity, certain actions are strictly prohibited. As a User, you may **not**:

- share your account or login credentials with others,
- use someone else's account or attempt to access data you are not authorised to access,
- upload or store data that are not related to research (e.g. administrative documents or private files),
- use the systems for activities that contravene applicable legislation, Aarhus University's internal rules, or research ethics standards,
- attempt to circumvent access control or other security features,
- undertake structured, automated or disproportionate data downloads, copying, transcription, photographing of data or other similar attempts to extract data from the Systems without legitimate cause or relevance to the research activity concerned,
- use scripts, robots, or other automated means to access or manipulate the Systems,
- install, run, or upload software that is not approved by Aarhus University,
- introduce malware, viruses, or similar malicious code into the Systems.

Suspected or confirmed violation of these Terms or other use unacceptable to Aarhus University may lead to:

- immediate restriction, suspension or permanent termination of access to the Systems,
- internal reporting to Aarhus University's security units or management,
- in serious cases: reporting to the police or assessment of legal liability.

Moreover, Aarhus University reserves the right, at its discretion, to restrict or terminate access to the Systems for any User whose conduct is deemed to be incompatible with the purpose or use of the Systems, regardless of whether there has been a breach of these Terms.

User behaviour and security

As a **User** you commit to:

- **complete the mandatory user course before being granted access, and comply with any local guidelines provided to you[1] [2],**
- **use the Systems in accordance with applicable legislation, including the General Data Protection Regulation, as well as Aarhus University's information security and research data management policies, including the ERDA and SIF guidelines,**
- **protect your login credentials and never share your account or access with anyone else,**
- **ensure that only authorised individuals with a legitimate purpose have access to research data in relevant project folders.**

[1] The course is administered locally. You can find your local coordinator here: https://medarbejdere.au.dk/en/administration/it/guides/datastorage/sif-at-au

[2] For more information on local guidelines, you can contact your system coordinator: https://medarbejdere.au.dk/en/administration/it/guides/datastorage/sif-at-au

All attempts at circumventing security measures, accessing data without authorisation, or otherwise using the Systems in violation of these Terms, are forbidden.

Violation of these rules and/or the Terms – including, for example, structured or automated downloads, or logging in from different IP addresses over a short period of time – may result in immediate blocking of access as well as possible involvement of relevant authorities.

Monitoring and logging

For security reasons and to protect both you and Aarhus University:

- all login attempts, instances of data access, and user behaviour, including time and user ID, are logged
- access patterns are automatically monitored, and suspicious behaviour may lead to temporary or permanent restriction or termination of access.

Examples of suspicious behaviour (non-exhaustive list):

- repeated login attempts from different locations within a short period of time,
- attempts to access data you are not authorised to access,
- automated or comprehensive data export.

Security breaches

All Users have a duty to take immediate action and report any suspected or confirmed security breach in connection with their use of ERDA or SIF.

Security breaches include (non-exhaustive list):

- unintentional access to data by unauthorised persons,
- sharing login credentials,
- suspicion that an account has been compromised or suspected data loss,
- download or manipulation of data without authorisation.

If you suspect a security breach, you must immediately:

1. **discontinue the activity and secure data if possible**, and
2. **report the incident** to the relevant contact:
    - For ERDA: erda-info.it@au.dk
    - For SIF: sif-info.it@au.dk
3. If applicable, **report the security breach** via one of these forms.

You can also inform your system coordinator at Aarhus University, if relevant.

Prompt reporting of security incidents is essential to minimising potential damage and complying with applicable data security and incident management regulations.

Access management and responsibility

Research coordinators at Aarhus University who grant access to others commit to:

- ensuring that the individuals concerned have completed the mandatory user course
- only granting access to Users who are actively associated with the project and who are able to comply with the security level requirements,
- continuously following up on access granted and immediately removing access that is no longer necessary, e.g. at the end of the project or upon resignation.

If you cease to be affiliated with Aarhus University, you must ensure that you transfer project and data responsibility correctly in accordance with Aarhus University's guidelines.

Duration and termination

Access to the Systems requires either active employment with Aarhus University, active affiliation with an institution engaged in research collaboration with Aarhus University, or active affiliation with a specific research project in ERDA or SIF in some other way.

Inactive external Users are automatically deleted after a period of one to three months after the end of the project, unless an extension has been agreed in writing beforehand.

The research coordinator is responsible for following up on the affiliation of Users to the project(s) for which they are responsible and ensuring that access is removed once it is no longer relevant. Aarhus University reserves the right to terminate access that no longer have a documented research purpose, or that is deemed a security risk.

Secrecy obligations and confidentiality

As a User of the Systems, you have a special duty to protect the data you access – especially when it comes to personal data, confidential third-party data, research results that will be patented, IP-protected material, or strategically sensitive research data.

You are therefore obligated to:

- **treat all research data in the Systems as confidential**, regardless of whether you are data controller or work on behalf of a research coordinator,
- **not to share, disseminate or disclose data to others** unless such sharing, dissemination or disclosure of data falls within the scope of the project's permissions, the data protection rules and Aarhus University's internal policies and guidelines,

- **comply with any separate confidentiality obligations** resulting from research collaborations, contracts, or legislation (including IP rights and export control),
- **ensure that data is not used for purposes other than those approved as part of the research project**, including that data may not be used in teaching or in other non-research contexts without separate, written approval.

Breaches of secrecy obligations and confidentiality can have serious implications and will be dealt with in accordance with AU's rules and staff policies. Aarhus University reserves its rights in all respects.

Disclaimer and system availability

Aarhus University makes the Systems available as campus solutions for storing and managing research data, but cannot guarantee uninterrupted access, full availability, or the suitability of the systems for all purposes.

The Systems are available "as is", and Aarhus University accepts no liability for, and cannot be held responsible for:

- temporary interruptions of service, including planned maintenance,
- data loss from User error, use of third-party software, misuse, or failure to backup outside of the standard functionality of the Systems,
- any consequences of the User's upload of data that is not suitable for or permitted in the Systems,
- direct or indirect financial losses, consequential damage, consequential or other derived effects and consequences resulting from the temporary or permanent restriction or termination of the User's access to the Systems,
- failure to comply with specific requirements beyond the specified functionality and security level of the Systems.

The User is personally responsible for:

- assessing whether research data is suitable for storing in ERDA or SIF respectively,
- ensuring the necessary legal basis for processing of the specific research data, and
- handling data in accordance with all relevant legal requirements, guidelines and the project's permissions.

In the event of errors or breakdowns, Users may inform the systems administration via the contact details at the bottom of this document.

Changes to Terms

Aarhus University reserves the right to update and amend these Terms (terms of use) on an ongoing basis and at any time to reflect changes in legislation, internal rules, system functionality, or security requirements.

Significant changes will be announced in advance as far as possible via:

- notices upon login to the Systems,
- direct emails to registered Users, or
- other relevant communication channels.

Users must keep themselves informed of the applicable terms. The continued use of the Systems following an update of the Terms will be taken to mean that the User agrees to the updated Terms.

The applicable version of the Terms will be available via the Systems' login page.

Governing law and venue

These Terms are governed by Danish law and must be construed in accordance with Danish law.

Any disputes arising out of or relating to the use of the Systems, including the construing or application of these Terms, must be settled by the ordinary courts of law with the Court of Aarhus as the legal venue, unless otherwise expressly provided by law.

Contact and support

If you have any questions about the use of the Systems, including access, technical problems, or security incidents, please contact the systems administration:

- **ERDA**: erda-info.it@au.dk
- **SIF**: sif-info.it@au.dk

Please include your name, username (AU ID), and, if possible, relevant project in your query.