Stockholms universitet

Terms of use for information systems and digital services at Stockholm University

General rules

Anyone who has been assigned a University account, or has in some other way been granted access to the University's information systems and digital services, is considered an authorised user. Passwords and other authentication data connected to University accounts are personal and may not be shared with any other person.

Authorisation is linked to the current employment or assignment and terminates automatically when this employment or assignment ends. Staff with extended rights or high authorisations must sign a special terms of use document with the University.

The basis for the terms is that information systems (computers, servers, networks, peripheral equipment) are owned by the University for use in the University's activities. Non-service-related use of the University's resources is only permitted to a limited extent when regular operations are not disrupted or when this is not in violation of applicable legislation or the University's rules and regulations.

In other respects, the following applies:

- all use of information systems and digital services must comply with Sweden's laws and ordinances,
- all computers, mobile devices and other equipment connected to the University's computer network must have adequate protection, such as antivirus protection, malware protection, firewalls or similar,
- information systems and services must not be used to view, download, print or otherwise handle pornographic or offensive material unless this is required by the work tasks,
- it is not permitted to conceal your identity when using information systems or digital services (such as, for example, use of the internet and email), unless this is required by the work tasks or is permitted by the freedom to communicate information or another statutory right under the principle of public access to official records,
- it is not permitted to exploit incorrect configurations, vulnerabilities or other methods to acquire extended system rights or other authorisations,
- copyrighted material may only be copied or distributed with the permission of the copyright holder. This means that it is not permitted to download copyrighted information or software without the permission or approval of the copyright holder,

IT Services
Stockholm University

Visiting address:
Universitetsvägen 10
106 91 Stockholm

Phone: +46 8-16 20 00

Stockholms universitet

- sedition, incitement to ethnic or racial hatred, sabotage and intrusion or attempted intrusion into local information systems or external systems are prohibited under applicable law.
- SUNET's ethical rules regulate other permitted use. SUNET condemns as unethical when anyone:
    - attempts to get access to network resources or other IT resources without having the rights to them
    - attempts to disrupt or interrupt the intended use of the network or connected IT resources
    - attempts to damage or destroy computer-based information
    - clearly wastes available resources (personnel, hardware or software)
    - violates the privacy of others
    - attempts to insult or demean others

Information classification

All information handled within the University's operations must be classified based on its security value. Information classification aims at ensuring that information is handled with the correct level of protection in terms of confidentiality, accuracy and availability.

The information classification forms the basis for how information may be stored, shared, processed and protected, as well as which technical and organisational security measures must be applied. The classification comprises both digital and physical information, regardless of medium or format.

Users of the University's information systems and digital services are responsible for:

- knowing and following the applicable information classifications for the information they handle,
- handling information in accordance with the rules decided for each information class,
- not sharing, storing or handling information in a manner that violates established classifications.

Information with a higher security value may only be handled in systems and environments that are approved for that information class. Aggregation of information may cause the information classification to be raised, even if the individual items of information have a lower security value.

In the event of any uncertainty in how information should be classified or handled, the user should contact the University's Section for Information and IT Security at IT Services before further processing of the information. Legal requirements always take precedence over internal security levels and classification decisions.