Stockholms universitet

2014-12-03

Reg. no. SU FV-1.1.2-3513-14

Benita Falenius
Information Security Coordinator

# Regulations for employees and personnel working on behalf of Stockholm University concerning the use of information and information management resources

Stockholm University 2014-11-28
IT Services Reg. no. SU FV-1.1.2-3513-14

## Target group

These regulations are aimed at employees at Stockholm University and people working on behalf of Stockholm University.

## Authorisation

Any person with a university account, or who has been granted access to the University's information or information management resources, is considered an authorised user.

Any associated passwords may not be shared with a third party. Under special circumstances, however, a password may be shared with the head of department/equivalent.

The authorisation is temporary and expires at the end of the employment, assignment, or similar.

The University signs written contracts with personnel with special authorisation within the University.

## General regulations

The basis of these regulations is that information and the associated information management resources (client computers, servers, networks, peripherals) are owned and managed by the University for use in University operations. Non-work-related use of University resources is only permitted to a limited extent:

- When regular activities are not disrupted;
- When it is not in conflict with applicable laws, University policies, provisions, guidelines, and regulations.

Stockholms universitet

Some information contained within the University may be regarded as official documents and thus constitutes public information. Personnel working with information security are responsible for monitoring the University's IT infrastructure and take action where necessary.

## Detailed regulations

- Information management resources may not be used to view, download, print, or otherwise handle pornographic or offensive material unless specifically authorised for work-related purposes.
- It is not permitted to hide one's identity when using information management resources (e.g. Internet and email), except where specifically authorised by the Vice-Chancellor or permitted in accordance with the freedom to provide information or other statutory rights under the principle of public access to official records.
- It is not permitted to exploit incorrect configurations, software bugs, or other methods in order to gain additional access or other privileges.
- All 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.
- Sabotage, sedition, incitement to racial hatred, and intrusion or attempted intrusion into local or external systems are prohibited in accordance with general legislation.

## Reports

Anyone who discovers faults, breaches, irregularities, or other problems, should report these to the head of department/equivalent.

Personnel with responsibility for information security should report breaches of internal regulations and applicable laws to the head of department/equivalent. The head of department/equivalent will determine, on the basis of the Public Employment Act, whether such a report should be referred to the disciplinary board or filed for prosecution. In other cases, the information security coordinator may take measures such as suspending accounts and restricting access to the University's information management resources pending further investigation.

Stockholms universitet

## CONFIRMATION

I hereby confirm that I have read the *Regulations for employees and personnel working on behalf of Stockholm University concerning the use of information and information management resources* and understand that it is my responsibility to comply with these regulations. I am aware that failure to comply with these regulations may result in the suspension of my account and access to the University's information management resources pending further investigation. In addition, it is incumbent upon me to notify the head of department/equivalent about any circumstances that will affect my access; for example, when my employment or assignment ends.

| **Date** | **Signature** |
|---|---|
| **Civic registration number** | **Name in block letters** |

Stockholms universitet

# Liability agreement for system administrators

This document is based on current legislation and the University's internal policy documents, which state that the responsibility for information security follows the delegation policy. It is the head of department/equivalent that is responsible for information security at each unit.

The head of department/equivalent can appoint an authorised user as a system administrator. A system administrator is a person with more privileges than regular users in IT systems and communication networks. The system administrator is typically responsible for the reliable operation and security of IT systems and networks, or involved in the operation or management thereof. The system administrator is appointed and granted privileges and obligations through a written decision by the head of department/equivalent. The decision should specify the systems or equivalent to which the privileges apply.

## Authorisation

Any authorised user can be appointed as a system administrator. A decision by the head of department/equivalent, in addition to a signed liability agreement, are required in order to be granted system administrator privileges.

| **Department/equivalent**: |
|---|

| **Name** | **Email address** |
|---|---|
| | |

| **IT resource** | **Comment** | **Term of appointment** |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Stockholms universitet

## Potential delegations

| Case | Term of appointment |
|---|---|
| | |
| | |
| | |
| | |

### Area of responsibility

It is assumed that the system administrator's responsibilities, powers, and obligations refer to all the unit's IT resources. If not, specify which IT resources are covered.

## Rights

On behalf of the University and in accordance with applicable laws, regulations, and decisions, the system administrator has the right to conduct the following actions:

- Monitor the resources he or she is responsible for and intervene without warning if necessary to secure the daily operation of the system or to perform troubleshooting;
- Suspend any user's access to IT resources in case of reasonable suspicion of unauthorised or improper use;
- Access and examine data when necessary to fulfil his or her duties. Permission from the head of department/equivalent is required in order to access and examine files and data.

## Incident management

The system administrator should:

- Document serious incidents and report them to the head of department/equivalent, or the person designated by the same, and the University's information security coordinator;
- Upon approval by the head of department/equivalent, take part in investigations concerning the unauthorised or unlawful use of resources;
- Have a procedure in place for dealing with incidents.

Stockholms universitet

## Obligations

The system administrator is obliged to:

- Follow the applicable guidelines and procedures for IT resources and information security at Stockholm University;
- Not disclose confidential information, except to law enforcement agencies;
- Supervise external personnel working on IT resources within the system administrator's area of responsibility;
- Report any suspected violations of applicable laws and regulations, primarily to the head of department/equivalent and the University's information security coordinator;
- Assist the head of department/equivalent, the University's disciplinary committee and information security coordinator, the Senior Management Team, and the head of IT Services during investigations of breaches of University regulations and applicable laws.

## Decision

The responsibilities, rights, and obligations mentioned above are delegated to the system administrator listed below.

| **Date** | **Head of department/equivalent Signature** | **Name in block letters** |
|---|---|---|
| | | |

Confirmation - I have read and accepted the terms listed above.

| **Date** | **System administrator Signature** | **Name in block letters** |
|---|---|---|
| | | |