Stockholms universitet

2014-12-03

Reg. no. SU FV-1.1.2-3514-14

Benita Falenius
Information Security Coordinator

Regulations for students and alumni concerning the use of Stockholm University's information and information management resources

Stockholm University 2014-11-28
IT Services Reg. no. SU FV-1.1.2-3514-14

Target group

These regulations are aimed at students and alumni 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.

The authorisation is temporary and expires at the end of the studies or when the user is no longer involved in alumni activities.

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. The use of University resources for purposes unrelated to studies or alumni activities is only permitted to a limited extent:

- When it is not in conflict with applicable laws, University policies, provisions, guidelines, and regulations.

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 taking action where necessary.

Stockholms universitet

Detailed regulations

- Information management resources may not be used to view, download, print, or otherwise handle pornographic or offensive material.
- It is not permitted to hide one's identity when using information management resources (such as Internet and email).
- 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 or the University's central Helpdesk.

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.