Linnéuniversitetet
Kalmar Växjö

User agreement for the use of Linnaeus University's computer, network and system resources

The aim of Linnaeus University is to ensure that its network is as accessible as possible. Computer resources, computer networks, related equipment and accounts are owned and managed by Linnaeus University for use in operations authorized by the university. Any other operations may only be allowed if they:

- Do not disrupt the regular use of resources.
- Do not constitute a breach of these regulations.
- Do not contravene the school's regulations, Linnaeus University's regulations, SUNET's regulations, or applicable Swedish law.

The term authorized is used in these regulations for persons who have been allocated an account, or otherwise have received permission to use Linnaeus University's computer, network or system resources.

For authorized users, the following regulations apply:

- Authorization and any associated resources may only be used by the authorized account owner.
- The password associated with the user identity shall be treated as a valuable item and is personal. See separate document for more information about password rules.
- Authorization will be terminated when the study period, appointment, project or equivalent has ended. Staff will continue to have read access for two months after employment has terminated.

The following applies to the use of Linnaeus University's computer, network and system resources:

- Sabotage or disruptive operations on the system or against other users, and unauthorized access or attempted access to the system, are strictly forbidden.
- It is not permitted to utilize wrongful configurations, programming bugs or other methods for the purpose of gaining access to more extensive system privileges or authorization other than allocated by the system owner.

Violation of the regulations will result in the following actions:

- Any suspected breach of our regulations is reported to the university's Incident Response Team (IRT): irt@lnu.se, http://irt.lnu.se
- The IRT then reports to the IT Security Coordinator who, in consultation with the IT Manager, makes a decision whether to escalate the case or not.
- The IT Security Coordinator reports to the Rector for further investigation.
- In order to secure the day-to-day operation, the system administrator (or someone on his/her behalf) has the right – within their area of responsibility – to monitor the university's systems and to check traffic or data which has been stored, in case of an incident.
- In case of a well-grounded suspicion that applicable regulations have been breached, the system owner has the right to deny access to Linnaeus University's computer, network and system resources in order to secure its operation. If the suspicion concerns a member of staff, this measure will be taken in consultation with the employee's direct manager.
- In case of an incident which forms a serious threat to the system, the system owner has the right to immediately deny access to Linnaeus University's computer, network and system resources in order to secure its operation.
- In case of a suspected violation of Swedish law, the authorities will report this to the police.

Applicable regulations can be found on the schools' notice boards, or electronically on Lnu.se.

I hereby pledge to keep up-to-date with, and follow, the regulations which are currently in force concerning the use of Linnaeus University's computer systems. I declare that I have read and understood these regulations.

I am aware that careless use, or failure to follow the instructions of those responsible for the systems, may result in access to the computer, network and system resources being denied. I am also aware that violations may result in legal proceedings and that any damages caused by such violations may lead to financial claims.

☐ Student ☐ Staff ☐ Guest

Date	Civic registration number	ID control (Not to be filled in by applicant)

Signature

Clarification of signature