



LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Data Administration and ICT Services
ICT Security, rule
13.5.2016
Public

E-mail rules of the University of Lapland

Ver- sion	Date	Modifications	Author
1.0	13.05.2016	Document created	Esa Mätäsaho
1.0	13.05.2016	Processed in the employee co-operation council	
1.0	16.05.2016	Approved by the Director of Administration	

1	E-MAIL RULES IN BRIEF	1
1.1	EVERY E-MAIL USER HAS ONE OR MORE ROLES	1
1.2	ALL RULES MUST BE OBEYED.....	1
1.3	STAFF MEMBERS.....	1
1.4	STUDENTS	1
1.5	MAILING LIST OWNER	1
1.6	SUPERVISOR.....	1
1.7	ORGANISATION ADDRESS OWNER.....	2
2	E-MAIL RULES.....	2
2.1	THE E-MAIL RULES COMPLY WITH THE CURRENTLY VALID LAWS AND REGULATIONS.....	2
2.2	PRIVACY OF CORRESPONDENCE ALSO APPLIES TO E-MAIL.....	2
2.3	E-MAIL ADDRESSES.....	2
3	USE OF E-MAIL AND E-MAIL ADDRESSES	3
4	SERVICE PROVISION AND ADMINISTRATION	5
5	OTHER CLAUSES	5

1 E-MAIL RULES IN BRIEF

1.1 EVERY E-MAIL USER HAS ONE OR MORE ROLES

- There are slightly different rules, for example, for staff members and students.

1.2 ALL RULES MUST BE OBEYED

- Use different passwords in the university services and in external services
- apply thorough consideration before using the university e-mail address for private purposes (see Rules of ICT Service Use)
- if you mistakenly receive e-mail intended for someone else, forward the message to the correct recipient, and inform the sender of the mistake
- remember that the privacy of correspondence also applies to e-mail
- make sure you have enough free space in your mailbox
- don't distribute spam
- don't leave any private messages in the university mailbox when your user rights expire.

1.3 STAFF MEMBERS

- Always use the university e-mail address for work-related correspondence
- send confirmations to e-service messages without any delay
- don't reroute work-related e-mail to external e-mail accounts
- keep your private and work-related messages separated, also the sent ones
- comply with the archive creation plan
- make sure your e-mail is monitored during your absence
- if you use an out-of-office message, instruct recipients to use the organization address
- only use e-mail encryption methods approved by the University
- if you are about to leave the University's employ, transfer all e-mail messages that are relevant for the organization to the responsible users before your user rights expire.

1.4 STUDENTS

- Use the university e-mail account for study-related purposes
- you can forbid the University from publishing your e-mail address
- all messages sent and received in the role of a student are private
- if you have an employment contract with the University, you are also bound by the staff members' rules; moreover, you must keep your work- and study-related e-mail clearly separated.

1.5 MAILING LIST OWNER

- Keep the list up to date (correct, valid addresses, brisk moderation)
- request the deletion of your list when it is no longer in use.
-

1.6 SUPERVISOR

- Make sure that all relevant organization addresses are available
- make sure that the organization addresses are used in your unit's communications
- appoint users responsible (with deputies) for monitoring the organization addresses.

1.7 ORGANISATION ADDRESS OWNER

- Establish procedures for message handling, back-up and informing other handlers
- change the password of the organization e-mail account regularly, and always after an e-mail handler (who knows the password) leaves the organization.

2 E-MAIL RULES

These e-mail rules concern all users of the University's e-mail systems. The parts aimed at staff members concern all of the University's units, their employees, and other corresponding users of the e-mail services. The rules also concern all users in charge of the e-mail systems.

2.1 THE E-MAIL RULES COMPLY WITH THE CURRENTLY VALID LAWS AND REGULATIONS.

The sender is responsible for making sure that the message delivery has been successful. Particularly crucial messages should be sent well before the deadline, and the recipient should be asked to confirm receipt.

2.2 PRIVACY OF CORRESPONDENCE ALSO APPLIES TO E-MAIL

If a user receives an e-mail message intended for another person, the unintended recipient is obligated to maintain the secrecy of the message and refrain from utilizing its contents or the knowledge of its existence.

- According to the Administrative Procedure Act (434/2003), Section 21, a document delivered by mistake and dealing with administrative matters beyond the recipient's competence shall be transferred to the authority deemed to be competent, and the sender of the document shall be informed about the transfer; if such a transfer is not possible, the message shall be returned to the sender and deleted from the university's e-mail system
- all other received messages intended for another user must be returned to the sender.

The forwarding and returning obligation does not concern messages containing malware or spam.

2.3 E-MAIL ADDRESSES

The organisation address is an official e-mail address

- The organisation address is used for official matters and service provision.
- For example: office@ulapland.fi

The work e-mail is a personal e-mail account provided for work-related use

- Example: john.smith@ulapland.fi
- Work e-mail messages are related to both the work e-mail account and the user's job.
- As default, the University considers e-mail messages received to the work e-mail account to be private messages.
- In outgoing e-mail messages, the organization address or the work e-mail address formed from the user's name must be given as the sender's address.

The study e-mail is a personal e-mail account provided by the University for its students

- Example: jsmith@ulapland.fi
- The study e-mail account is primarily intended for study-related use.
- The University considers students' e-mail messages to be private messages.

- The sender's address in outgoing e-mail messages is the study e-mail address formed from the student's name.
- Every e-mail service user is personally responsible for keeping his/her mailboxes clean and ensuring that the reserved space does not run out.

The University determines the e-mail addresses and their format

- All e-mail addresses are based on the names of the users.
- Staff member addresses typically contain the user's first name and last name.
- Student addresses do not follow the firstname.lastname logic. Instead, they typically contain the initial letter of the first name followed by the first seven letters of the last name – unless the last name is shorter.

3 USE OF E-MAIL AND E-MAIL ADDRESSES

- The name-based address must be used as the personal e-mail address
- the organization addresses are used in the university's communications]
- the organization address or work e-mail address must be used in work-related matters.

The handling and archiving of e-mail messages received to the organization or work e-mail account are governed by the Act on the Openness of Government Activities and the university's archive creation plan.

- It is forbidden to transfer or automatically route e-mail messages from the organization or work account outside the University; this is due to reasons related to information security, data protection and information management; in addition, it may constitute a breach of the Personal Data Act
- if a received message contains a confirmation request or is part of an e-service ¹, the message handler must send the confirmation immediately
- only e-service systems are allowed to use automatic receipt confirmations.

Organization addresses have owners

The owner must make sure that messages received in the organization address are handled on a regular basis and according to the archive creation plan, even when the owner is absent.

- E-mail messages received in the organization account belong to the employer
- the address owner must respond to any received messages immediately
- the response must indicate that it is a reply to a message sent to an organization address
- organization addresses must not be used for personal communications.

Messages related to work e-mail accounts are treated as private messages

- The University can retrieve and open an employee's e-mail messages in certain cases and certain ways as defined in separate guidelines.
- work-related e-mail messages sent by employees must, when applicable, clearly indicate whether they are official statements related to work or the employee's personal opinions
- when responding to applications or other such matters related to public administration, the response message's reply address must be an organization address
- instead of changing the reply address, the sender can be advised to use the organization address in the future
- the original message and the response are transferred to the organization address for archiving.

¹ Here, the term 'e-services' refers to the electronic registration, completion and processing (incl. resolution) of administrative matters, informing about decisions, or sending a trial document in electronic format to a public court or to a person authorised by such an instance.

The e-mail account provided by the University can be used for private purposes within the limitations set forth in the university's Rules of ICT Service Use.

- Employees must clearly separate their personal and work-related e-mail messages, both those received and sent
- if a user is both a student and a staff member, the e-mail messages related to each role must be clearly separated from each other.

External e-mail accounts must not be used for university-related tasks

Access to external e-mail services from the university network can be technically restricted, if such services are deemed to form a major data security risk.

Use personal auto replies with caution

Auto replies entail a risk of spam flow, but if one is nevertheless deemed necessary, it should advise the recipient to contact the relevant organization address.

E-mail must be monitored even during absence

One option is to close the mailbox (for example, during long leaves of absence). The recommended practice is to instruct clients to use the respective organization address for all contacts.

The e-mail account is fixed-term

Personal messages should not be left in the university mailbox when the usage right expires.

Employees must agree with their supervisor on the transfer of work-related messages to another user within the university organization. If an employee resigns from his/her duties before the expiry of the employment contract, the employee, or his/her supervisor, can request the discontinuation of incoming e-mail immediately.

E-mail messages can be encrypted

All applications used for encrypting organization- and work-related e-mail messages must be approved and implemented by the University.

- If a received organization- or work-related e-mail message is encrypted so that only the recipient can decrypt it, the message must be decrypted immediately after receipt; this rule does not apply to messages containing malware or spam
- after decrypting, the message can be encrypted again so that all handlers can open it.

In terms of information security, non-encrypted e-mail can be compared to a postcard.

Mailing lists have owners

The owner must keep the list moderated, regularly check that it is up-to-date and remove any redundant addresses from the list.

- The list owner is responsible for maintaining and removing joint mailing lists.
- Personal mailing lists are each user's own responsibility.

A mailing list forms a person register and, hence, it may be subject to confidentiality obligations and separate limitations of disclosure. If such rules apply, use the blind carbon copy (bcc) function in order to keep the list's addresses hidden from recipients.

Mass mailing and sending/forwarding chain letters is forbidden

Exceptions to this rule can be made upon separate decisions.

4 SERVICE PROVISION AND ADMINISTRATION

System administration can intervene in e-mail traffic

in order to secure the service level or safety of the e-mail system. Such interventions, as well as e-mail usage monitoring and log-keeping, are governed by separate instructions.

E-mail is checked and filtered

All e-mail traffic goes through an automatic content analysis, based on which

- messages and attachments containing malware are automatically deleted
- the delivery of harmful, oversized or numerous attachments can be restricted.

In addition, filtering and deletion without notification can be applied to messages

- sent from known spam servers
- classified as spam based on the automatic content analysis.

The e-mail address no longer works

when the usage authorization has expired. Messages sent to a user whose e-mail account is no longer valid will not be delivered; instead, an automatic message is sent to inform the sender about the expiry of the address. When an e-mail account expires, all its re-routing arrangements also become invalid.

5 OTHER CLAUSES

Validity

These e-mail rules become effective 16 May 2016 and replace the earlier version of corresponding rules.

Change management

These rules will be reviewed when needed to ensure that they comply with all valid services and laws. Any significant personnel-related changes are addressed according to the co-operation procedure. The Chief Information Officer of the University of Lapland makes the decisions concerning change needs.

Information about changes is distributed using the regular communication channels, never personally.

Deviations from the e-mail rules

Permission for exceptions from the e-mail rules can be granted for compelling reasons upon a written application. Special permits are granted by the Chief Information Officer of the University of Lapland. The permits may include additional terms and conditions, restrictions and responsibilities.

Monitoring

Compliance with the e-mail rules is overseen by the ICT Security Manager of the University of Lapland in cooperation with the ICT Services of the Service Center of the Lapland University Consortium, as well as by superiors within their job descriptions. Breaches of the rules lead to sanctions according to the applicable Legislation.

The rules will be upgraded when needed. The need for upgrading is monitored by the ICT Security Manager.

Further information

The rules and instructions concerning the ICT services are on the [website of the University of Lapland](#).