Directions for e-mail at KTH

Valid from 2010-07-01

- desicision UF-2010/0299

Aim

The aim of these directions is to collate information on the design of the central e-mail system and how it is intended to be used, how spam, antivirus and backup are managed, instructions on the management of mass circulation, what phishing is and its consequences. Amednments to this document are decided by the e-mail group authorised by the IT management group. For general rules and an outline of the legislation on which the rules are based, see Regulations for e-mail at KTH. The rules in the Regulations have precedence over these Directions.

Functions of the e-mail system

The central e-mail system consists of a number of functions that are dispersed across several severs in various computer rooms. The e-mail system must function even if one of the servers has ceased to function. The system consists in principle of two different parts. One incoming/outgoing e-mail flow (MX/SMTP), and a system where e-mails are stored where users are given the opportunity of reading and sending e-mails (Exchange). A sketch is given below.

Those functions depicted are

- MX/SMTP – Incoming e-mail flow
- MX/SMTP – Outgoing e-mail flow
- Backup
- E-mail for users (Exchange)

MX/SMTP

Incoming e-mail flow

Central e-mail addresses have the form “*@kth.se”. The system consists of two main elements: MX and Exchange.

The MX layer consists of the following functions:

- Whitelisting
- Greylisting
- Antivirus control
- Spam tagging
- Delivery to internal/external e-mail server

E-mail arrives first at greylisting. The e-mail that passes greylisting continues on to amavis for virus and spam control. Spamassassin is used for spam tagging. If the e-mail is assessed as being spam, it is placed in quarantine and delivered to a separate mailbox.
After the mail has passed the above stratum, it is delivered to the internal/external e-mail server.

The deivery process utilizes LDAP (transport map) and UG:s specification to determine the recipient´s adress and it´s destination.

The exchange servers at KTH only receive e-mail from MX/SMTP.

Outgoing mail flow

The smtp layer consists of the following components

- User/system
- smtp.kth.se
- Antivirus control
- Spam tagging
- Delivery to internal/external e-mail server

The users and systems send outgoing e-mails through smtp.kth.se for anti-virus control and spam tagging before delivery to an internal/external server. Users can also send mail using smtp/a (authenticated smtp) through smtp.kth.se, which is always recommended. Smtp.kth.se allows you to send e-mail through smtp.kth.se anonymously if you are working locally on the KTH network (excluding kthopen/eduroam).

Backup

E-mail data is backed up three times each day. The backup is saved on disk for 90 days. Reinstalling data today consumes considerable time and resources and is only carried out in exceptional cases. The product we use is Microsoft Data Protection Manager (DPM). Apart from this data is left in the mailbox for 20 days, even if it has been deleted.

Exchange

Exchange is an e-mail system consisting of servers with various types of function, such as database, client access and e-mail transport. All the information in the database is saved in the mailbox. Currently we have 36 databases, dispersed across the system where e-mail are stored. 3 clusters (active – passive) have been defined.

The client access function delivers information to the client via the web, imap, pop and activesync. The e-mail transport function is the part delivering e-mail in and out of the system and between users.

Spam/Virus/Phishing

If you suspect that your username and password are being misused by other people, contact IRT

abuse@kth.se

It is important never to give your username and password to anyone. No office within KTH will ask you for your password. In case of uncertainty, always contact IT-SupportCenter.

General about spam

Spam is a name for junk mail; It is undesirable e-mails sent out in huge mass circulations advertising various products and other products sold off cheaply or more or less sensational topics to interest the receipient. There is often a financial motive; it is cheap to spam. It does happen that KTH's computers are used by spammers to forward on their mails. This can lead to other operators blacklisting KTH.SE; it is of great importance that we counteract spam from both external and KTH systems so that we are not part of the chain which spreads the spam. Undesirable e-mail may be reported to KTH IRT for further action. It is also possible to whitelist recipients so they receive all the spam, which is, for example, important when it is a question of departmental addresses. There is also the possibility of rewriting subject areas for those domains that wish to do so, for example (SPAM).

It is possible to whitelist sending e-mail servers and sending addresses.

The effects of spam

Spam delays legitimate mail and sometimes causes it to "drown in the flood". Components of the e-mail system to counteract spam:

- Spamassassin is used for spam tagging, that is to say it allocates points. If an e-mail is allocated more than five points then it will be tagged as spam with the flag: "X-Spam-Flag: YES". An e-mail with more than five points is weeded out and ends up in a central "spam box". Users will themselves have to contact postmaster@kth.se in order to get all their spam-tagged e-mails into their inbox. Spamassassin uses four sets of rules, such as KTH's rules, bayes, razor (external service) and spamassassin's own rules.
- Grey listing is used by KTH to counteract spam. This is based on the user fully supporting re-sends according to "RFC 5321" para."4.5.4.1", which many systems sending spam will not do.

postmaster@kth.se

When a receiving server recieves e-mail, it checks its memory for the combination “Sending computer -> sender address -> recipient address”. If it cannot find the combination, it will save it in memory and respond to the sending computer that there has been a “Temporary fault”. Now the e-mail is on the so-called greylist. The sending computer should then, according to “RFC 5321” para. “4.5.4.1”, attempt to send the e-mail again. In this resend, where the combination “Sending computer -> sender adress -> recipient adress” is identical with the previous attempt, the receiving server will remember the combination and answer OK. The e-mail has now passed the greylist and the combination is able in the future to send e-mails without temporary faults. The time the combination has to spend on the grey list is normally 60 seconds. But if the sending computer is on an RBL (Real-time Blackhole List) it spends 1,000 seconds on the greylist. Automatic white listing occurs on the sending computer. Real e-mail servers which do not process resends do exist; these can be whitelisted manually, so that they are not affected by greylisting.

Greylisting works in such a way that, if the system has not previously encountered the combination “sender -recipient - sending network (/24)”, then the KTH e-mail little system sends a temporary fault message to the sending e-mail server and asks it to try to send the mail later. This is to stop spam attacks.

Measures

In order to reduce the risk of being affected by spam attacks and to minimise the damage, certain measures are necessary. Some examples of these are:

- Blocking/filtering/quarantine of incoming and outgoing suspect mails with the aid of suppression lists - local or public
- Detection and alarm when an outgoing spam attack is in progress
- Delay of mail of this kind through so-called “throttling”
- Detection and alarm for incoming phishing or similar messages
- Opportunity to clean user’s mailbox from verified spam messages
- Opportunity of rapidly detecting a spam attack through the user’s account and blocking the account, cleaning queues etc.

Antivirus

By virus, “malignant code”; software contains functions unknown to the user, thus undesirable from a safety point of view and it has been consciously inserted by the creator. All central e-mail is inspected with the aim of discovering viruses, worms, spyware and malware. In the first place this will be removed from the message. If this fails, the mail will end up in so-called quarantine.

Description– virus/malware

Examples of the functionality of a virus/malware may be to log all the keystrokes the user makes (with the aim of capturing passwords and other sensitive information), to destroy stored information, or to make it possible for the computer to be used for sending out spam, or some other form of misuse.

Countermeasures – virus/malware

There are a number of different methods and tools you can use to protect yourself against malware. It is, however, important to understand that it is only a combination of the correct tools and a large measure of care that provides good protection. As an ordinary computer user, or a system administrator you cannot simply trust the computer's basic safety functions, but also have to combine antivirus software, anti-spyware program, firewall and sound scepticism to avoid problems. The technology does not protect us unless we are cautious when we surf the Internet. A good way of protecting yourself against problems is to combine firewall, antivirus program, anti-spyware program and also implement latest version of operating system combined with a large measure of care and common sense. None of those programs are all-embracing, different software producers differ rapidity with their release virus/spyware definitions. Everybody using the central e-mail system should have an anti-virus client installed irrespective of their operating system.

Components of the e-mail system to counteract viruses

Virus control in the MX layer. E-mails containing viruses or prohibited files are saved in quarantine on each MX server, and sent to a departmental mailbox at Exchange. E-mail with attachments of the type exe, .com, .pif, .scr, .bat, etc. are automatically discarded.

Virus control at Exchange exists in two parts, one on incoming/outgoing in the e-mail transport and two, on the database servers. In Exchange there is access to five different antivirus engines for detecting viruses. Encrypted zipfiles and compressed files are treated as suspect and saved in quarantine locally on the server. Corrupt compresed files are discarded on detection.

Phishing management

Phishing means a method of deceiving another person into revealing confidential details such as, for example, account numbers, credit card numbers, passwords etc. The commonest deception involves contacting the victim via e-mail, as this is the cheapest and most effective method of reaching a large number of people. The mails are often designed to look as if they come from a bank or an IT support organisation. The language used to be poor, but this has changed and the mails are now relatively well written.

Effects of phishing

When the attempt succeeds and the victim sends off their details, several different things may happen. The most common as regards the account/credit card number is, of course, that an attempt is made to transfer money or pay using the information acquired. In the case where the account/password is sent, it is common that the relevant account is used to send out large numbers of new phishing messages or spam. In the context of more targeted attacks, account information is used to steal information or continue hacking.

Countermeasures against phishing by e-mail

It is not so simple to protect yourself against this type of fraud. The most important things is, as usual, to inform the users so that they never send sensitive information via e-mail. Various kinds of suppression lists can be established with e-mail addresses that we know are used in connection with phishing attacks, either personal or public addresses which can be downloaded. The problem of this method is that a large number of messages have often had time to enter the system before the relevant addresses appear in the suppression lists. When an address has ended up on a suppression list, the e-mail system will no longer send e-mail to or from the suppressed addresses, which means that the phisher cannot contact his victims, and anyone attempting to respond cannot send out information. One problem in this regard is the fact that there is often no control of an e-mail user's outgoing communications – they can for example be managed from the user's home network, which not unusually means that the mail is sent via the nearest e-mail server in the relevant ISP.

For this reason, it is not possible to know with certainty which users who have responded to phishing expeditions.

Components in e-mail systems to counteract phishing

In order to reduce the risk of being subjected to phishing attacks , and that users respond to these, and to minimise the damage, certain measures are required. Some examples of these are:

- Blocking/filtering/quarantine of incoming and outgoing phishing mails with the aid of suppression lists – local or public
- Detection and alarm when a user responds to a phishing message
- Detection and alarm on incoming messages of phishing type
- Opportunity of cleaning a user's mail boxes of confirmed suspect messages
- Opportunity of rapidly detecting a spam attack via the account of a deceived user and suppressing the account and cleaning the queues etc (see also under SPAM) Virus/malware
- System administrators and users at KTH may report suspect phishing on the IRT portal, where there are also lists of suppressed sender addresses

Using e-mail at KTH

The central e-mail system automatically creates mailboxes for all employees and students at KTH. Mailboxes are created when the account is generated in the central user database UG.

Types of e-mail address

Personal addresses

A personal address is linked directly to a specific individual.

Group addresses/Distribution list

A group address is the address of all the members in the group.

Departmental addresses

Departmental addresses are e-mail addresses to a certain department instead of to specific individual. Departmental addresses at KTH, see Appendix 1.

Absence management

All employees have the responsibility during any absence to manage their mailbox according to one of the following alternatives:

- Activate an e-mail out-of-office autoreply system. State the time of your absence, contact details to colleagues and/or the school's registrar and refer to the relevant departmental mailbox
- Activate automatic forwarding to a colleague or to the registrar of the school
- Allocate your mailbox to a colleague
- Monitor your mailbox yourself

If documents from a private mailbox are requested and the employee is not available because of holiday, illness or for other reasons it is incumbent on KTH's IT administration to forward mail to KTH's central registry, which then manages the handover. Forwarding to the registry is carried out at the request of the person who has received a request for surrender of the document. IT support is responsible for KTH's central e-mail system for forwarding. The method also applies in other situations where access to an employee's e-mail in the case of their absence is required in order for KTH as an authority to be able to meet its responsibilities.

Signatures

A common signature for KTH's employees has been compiled for KTH. See references

E-mail addresses

At KTH there are a number of different types of addresses which are to be used. Which addresses it is possible to use and which rules we are to follow. For current shared mailadresses, see Appendix 1

Address space

- Personal e- mail addresses consist of 2-8 characters including a-z, 0-9. The address must not begin with the letter "u" followed by a figure.
- E- mail addresses consisting of more than eight characters or up to 8 letters (no figures) in combination with a minus sign "-" or underscore "_" are reserved for group and departmental addresses
- Addresses in the standard format or organisational format where recipients correspond to the format of a course code or similar are reserved for group addresses
- Addresses, irrespective of format, where the recipient is a generally accepted concept for a department, are reserved for departmental addresses.
- Exceptions from the above can be permitted by the e-mail group.

Prohibited addresses

- Addresses in the standard format where the recipient consists of a first name combined with a surname are not allowed
- Addresses, irrespective of format, where the recipient contains characters other than the letters ‘a’ to ‘z’, figures and a dot ‘.’, minus sign ‘-‘ or underscore ‘_’ are not allowed.
- Addresses, irrespective of format , where the recipient is a word which might be considered to be objectionable or have a political, religious or discriminatory sense are not allowed.
- Addresses coinciding with names of commonly occurring system accounts, systems, reserved words in systems, protocols, services, e-mail aliases, shared addresses and addresses in UG’s list of forbidden addresses are not allowed.
- Addresses should consist of at least two characters. If there are exceptional reasons , exceptions can be allowed by the e-mail group.
- Exceptions are made for certain older addresses

Mailboxes

Central e-mail system consists of three different types of mailboxes.

Personal mailboxes

The mailbox of a private individual linked to a personal address.

Shared mailboxes

A mailbox that is impersonal, means a mailbox which several people can read and send from. This mailbox is linked to a shared address. It can be read by or answered by one or several individuals. The advantages of shared addresses are among other things:

- Several people can monitor and process mail to the department irrespective of holidays, changes in personnel etc.
- Standardised shared addresses provide natural and easily remembered way of communicating with the authority’s departments.
- Registration and other processing of incoming e-mail is facilitated by the use of shared addresses. It is preferable that e-mail addressed to shared mailboxes should be processed with the aid of a case management system.

Shared calendar

An impersonal mailbox whose function is to be a calendar in the central e-mail system. An example of this may be a booking calendar for a conference room or for a loan projector.

Quota

All users have as a standard 2 GB of space in the e-mail system. Extra space is granted for employees after consultation with the IT-Supportcenter. No more space is allocated if the majority of the space consists of private e-mails. The IT-Supportcenter has the right of increasing the quota up to 5 GB; for anything in excess of this quota the system group should be contacted.

Phasing out mailboxes

Mailboxes will remain until further notice.

When a member of staff leaves the university, the account will be removed from all groups so as subsequently to be given the affiliation alumnus.

Directions for mass circulation

In mass circulation one should consider who is the target group and who needs to read the e-mail message. It is not always all recipients who consider that the information is relevant/interesting. Is the content in any attached document really of interest to the reader, or could it be communicated in a quicker and simpler way in the text of a mail? For this reason the following apply to circulations with more than 20 recipients.

- Aim, target group and source address should be clear in the mail.
- Mass mailings for marketing purposes or advertising purposes are not permitted, not even for non-profit activities.
- It is not permitted to send e-mails containing political, religious, racist or sexist propaganda.
- The language in the mail should be kept at a level that is not regarded as irresponsible.
- A private recipient should not be able to see other e-mail addresses the mail has been sent to.
- The sender should be address@kth.se
- If there is any doubt or questions, contact postmaster@kth.se before despatching the mailing. If the mailing is considered to be legitimate, then the sender will be given a signature to append to the mailing where it is clearly stated that the content has been scrutinised and approved by the postmaster.

Write “For information ” if the recipient is not expected to act on the e-mail. Alternatively, a copy of the e-mail message can be sent, which signals that the mail has been sent for information.

KTH’s intranet should be used for larger target groups. Remember that the intranet is better suited for many general types of messages, notices of meetings, minutes, etc., where the target group is an entire working party, department or administration. Do not send jokes, chain letters, begging letters and the like in an official capacity, irrespective of how deserving the aim may be felt to be.

Despatching mails to a large number of recipients in a short period will automatically send an alarm to IRT. Whitelisting is possible, and is carried out according to an established routine.

How do you make a mass mailing?

In order for large mailings not to get caught in the spam quarantine, you should first contact IT-SupportCenter; then your address will be whitelisted at the time you make your mailing. You then send an e-mail to

it-support@kth.se

in the mail you describe which address you are sending from and when you are going to make your mailing.

Junk e-mail

Everything to be found in the Junk Mail folder is to be regarded as not weeded, that is to say still a public document, and will automatically be deleted after 365 days.

Waste paper basket

Everything to be found in the waste paper basket (Deleted Items/Trash) is to be regarded as not weeded , that is to say still a public document and will automatically be deleted after 365 days.

Address books

All employees and students are to be found in the global address book. Anyone who has a central mailbox has access to this. In LDAP all employees' telephone numbers and the address of their workplace are to be found. This is approved for publication when you sign your letter of undertaking.

Access to the central e-mail system

There are a number of different ways of accessing your mailbox in the central e-mail system:

- IMAP
- MAPI for Outlook
- Outlook anywhere (RPC via https). The technology for running Outlook outside KTH's network without needing to run vpn (supported by Outlook 2003 and later).
- POP 3
- Webmail
- Webservices (for, among others, entourage and mail on mac)
- Kalender
- Autoconfiguration for clients (Outlook 2007 and later)
- Exchange active-sync for mobiles/smartphones

On how to configure your client you can find further information from IT-SupportCenter.

intra.kth.se/it/it-support/it-sc

Personal integrity in the e-mail context

The letter of undertaking sets out what is permissible for IT staff to do with the content of an mailbox.

PUL

When you sign your letter of undertaking this means that your personal details will be found in the KTH system.

Alumni

Alumni are allowed to have e-mail accounts.
See references.

The IT department's routines when someone dies

The system group's measures

Deactivate computer account
Remove name from address list in Exchange/LDAP

- Deactivate computer account
- Remove mailbox
- Archive mailbox to home catalogue

Concepts

Alias – An alternative name for a user and an e-mail address.

User – A unique individual who has access to one or more KTH's computer resources.

KTH account – A unique identifier of the user.

Postmaster – An office with responsibility for informing, planning, maintaining and developing the e-mail system/storage. Administers e-mail servers and ancillary systems.

Quota – The space allocated for e-mail to an individual user.

Junk mail/spam – Unwanted e-mail.

Waste paper basket/Deleted items – Space for deleted e-mails.

Shared address – An e-mail address of a particular department, e.g.

registrator@kth.se

RFC – Request For Comments is a document describing a standard. For further information about RFC see:

www.ietf.org/rfc.html

Alumnus - Former employee or student.
Standard format – E-mail addresses in standard format:

recipient@kth.se

Organisational format - E-mail addresses in organisational format:
recipient@organisation.kth.se These addresses are associated with and/or delegated to an organisation at KTH

Questions will be sent to:

postmaster@kth.se