ANVISNING

Gäller från och med
2011-10-11

Anvisning för e-post vid KTH

Gäller fr o m 2010-07-01
Uppdaterad 111011

Anvisningen grundar sig på:

- Rektorsbeslut UF-2010/0299, Dnr V-2010-0343, Doss 10

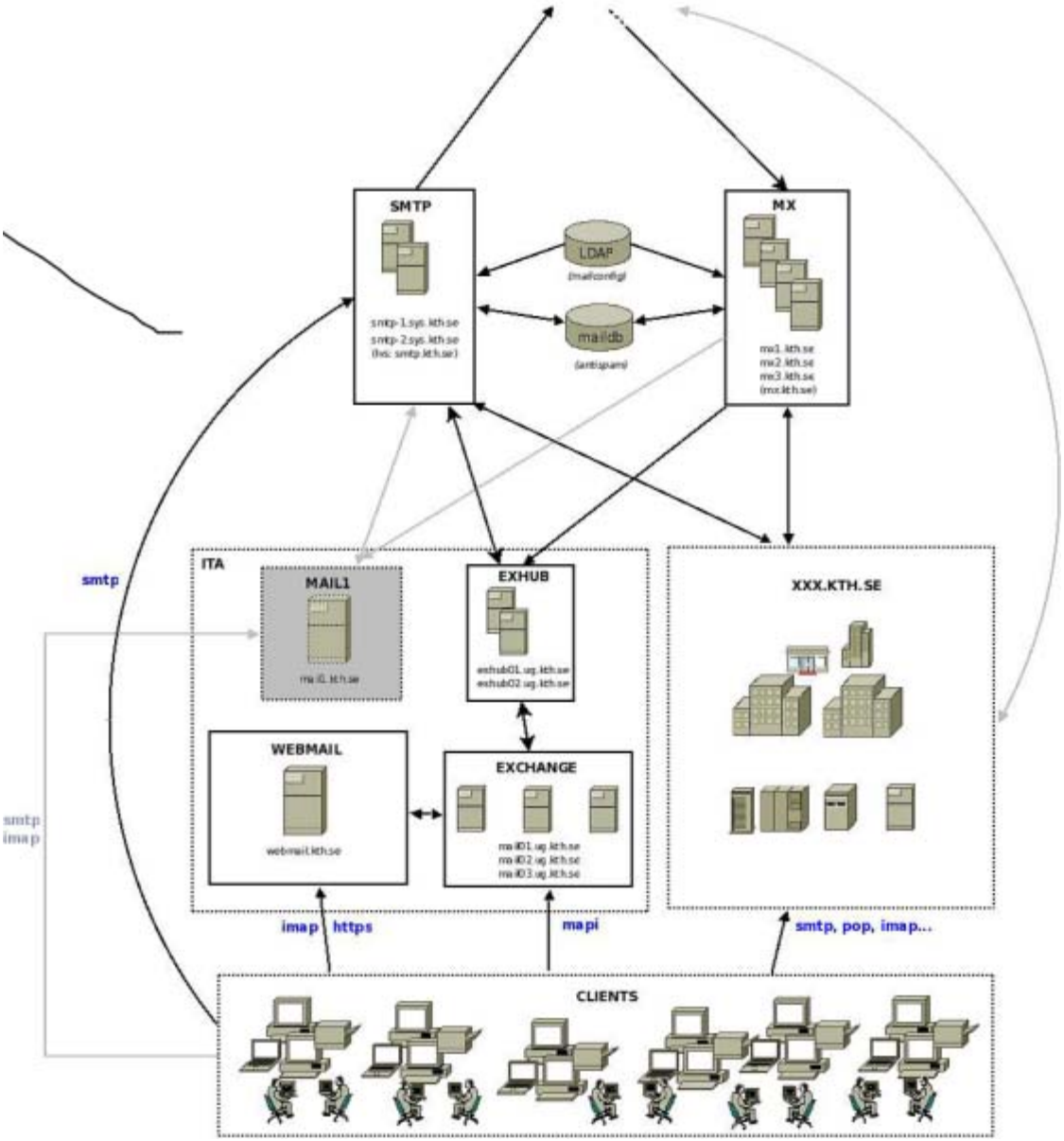
Syfte

Syftet med denna anvisning är att samla information om hur det centrala e-postsystemet är uppbyggt och är tänkt att användas. Hur spam, antivirus och backup hanteras. Instruktioner om hantering av massutskick, vad phishing är och vilka konsekvenser det kan få.
Förändringar i detta dokument beslutas av e-postgruppen på delegation av IT-ledningsgruppen.

För övergripande regler samt en översiktligt beskrivning av lagstiftning som reglerna grundar sig på, se Föreskrift för e-post vid KTH. Reglerna i föreskriften har företräde framför denna anvisning.

Funktioner i e-postsystemet

Det centrala e-postsystemet består av ett flertal funktioner som är spridda över ett antal servrar i olika datorhallar. E-postsystemet ska fungera även om någon server slutar fungera. Systemet består i princip av 2 olika delar, ett inkommande/utgående e-postflöde (MX/SMTP) och dels ett system där e-posten lagras och där användarna ges möjlighet att läsa och skicka e-post (Exchange). En schematisk skiss ses nedan.



De funktioner som beskrivs är

- MX/SMTP – inkommande e-postflöde
- MX/SMTP –Utgående e-postflöde
- Backup
- E-post för användarna (Exchange)

MX/SMTP

Inkommande e-postflöde

Centrala e-postadresser har formatet"*@kth.se". Systemet består av 2 huvudkomponenter: MX och Exchange.

MX-lagret består av följande funktioner:

- Whitelisting/vitlistning
- Greylisting/grålistning
- Antiviruskontroll
- Spamtaggning
- Leverans till intern/extern e-postserver

E-post kommer först till grålistningen. E-post som klarar grålistningen går vidare till amavis för virus- och spamkontroll. Spamassassin används för spamtaggning. Bedöms e-posten vara ett spam så placeras det i karantän och levereras till en separat e-postbox.

När brevet passerat ovanstående lager så levereras brevet till intern/extern e-postserver, detta är baserat på regler i LDAP (transport map) och vilken mottagaradress brevet fått genom tidigare uppslag i UG.

Exchange-servrarna på KTH tar endast emot e-post från MX/SMTP.

Utgående e-postflöde

- Användare/system
- smtp.kth.se
- Antiviruskontroll
- Spamtaggning
- Leverans till intern/extern e-postserver

Användare och system kan skicka utgående e-post genom smtp.kth.se för antiviruskoll och spamtaggning innan leverans till intern/extern server. Användare kan också skicka med smtp/a (authenticated smtp) genom smtp.kth.se vilket alltid är att rekommendera.
Smtp.kth.se tillåter att man skickar e-post genom smtp.kth.se anonymt om man sitter lokalt på KTH:s nät, (exkl. kthopen/eduroam).

Backup

E-postdata backas upp 3 ggr per dag. Backupen sparas i 90 dagar på disk. Att lägga tillbaka data är idag både tids och resurskrävande och görs endast i undantagsfall. Produkten vi använder är Microsoft Data Protection Manager (DPM). Utöver detta ligger data kvar i e-postboxen i 20 dagar även om man tagit bort den.

Exchange

Exchange är ett e-postsystem som består av servrar med olika typer av funktoner såsom databas, klientaccess och e-posttransport.

I databasen sparas all information i e-postboxen. Vi har idag 36 databaser som är spridda över de delar där e-posten lagras och de består av 3 stycken kluster (Aktiv-passiv).

Klientaccessfunktionen levererar information till klienterna via web, imap, pop och activesync.

E-posttransportfunktionen är den del som levererar e-post in och ut ur systemet samt mellan användare.

Spam/Virus/Phishing

Vid misstanke om att ditt användarnamn och lösenord missbrukas av andra kontakta IRT

abuse@kth.se

Viktigt är att aldrig lämna ut ditt användarnamn och lösenord till någon. Inget driftställe på KTH kommer att begära ut ditt lösenord. Vid oklarheter kontakta alltid IT-SupportCenter.

Allmänt om spam

Spam är benämningen på skräppost, dvs. oönskad e-post som skickas ut i stora massutskick med reklam för diverse produkter och andra slumpade eller medvetet sensationella ämnen för att intressera mottagaren. Det finns ofta ett ekonomiskt syfte bakom, det är billigt att spamma. Det händer att KTH:s datorer används av spammare för att vidarebefordra utskick. Detta kan leda till att andra operatörer svartlistar KTH. SE, det är av högsta vikt att vi motverkar spam från både externa operatörer och KTH:s system så att vi inte är med i spridningskedjan.

Oönskad e-post kan rapporteras till KTH IRT för vidare handläggning. Det går även här att vitlista mottagare så de får all spam vilket t.ex. är viktigt då det handlar om funktionsadresser. Det finns även möjlighet att skriva om ämnesraden för de domäner som vill det, exempelvis (SPAM). Det går att vitlista avsändande e-postserver och avsändaradress.

Effekter av spam

Spam fördröjer och får ibland legitim e-post att "drunkna i floden". Komponenter i e-postsystem för att motverka spam

- Spamassassin används för spamtaggning, dvs. den poängsätter e-post, om e-post får mer än 5 poäng så kommer det att taggas som spam med flaggan: "X-Spam-Flag: YES", e-post som klassa med mer än 5 poäng gallras bort och hamnar i en central "spamlåda". En användare måste själv kontakta postmaster@kth.se (se nedan) för att få all sin spam taggade e-post till sin inbox. Spamassassin använder fyra regelverk, dels KTH:s regler, bayes, razor (extern tjänst) samt spamassassins egna regler.

postmaster@kth.se

- Grålistning används av KTH för att bekämpa spam, det bygger på att användaren till fullo stöder omsändningar enligt "RFC 5321" stycke "4.5.4.1", vilket många system som skickar spam inte gör.

Vad som sker är att, när mottagande server börjar ta emot e-post så kollar den i sitt minne efter kombinationen, "avsändande dator -> avsändar-adress -> mottagar-adress". Finner/minns den inte kombinationen kommer den att spara den i minnet och svara avsändande dator att det uppstått ett "Temporärt fel". Nu befinner sig e-posten i den s.k. grålistan. Sändande dator ska då enl. "RFC 5321" stycke "4.5.4.1" försöka skicka e-posten igen. Vid denna omsändning, där kombinationen "Sändande dator -> avsändar-adress -> mottagar-adress" är identisk med föregående försök, kommer mottagande server minnas kombinationen och svara OK. E-posten har nu passerat grålistan och den kombinationen får fortsättningsvis skicka e-post utan temporära fel. Den tid kombinationen måste befinna sig i grålistan är normalt 60 sekunder. Men är sändande dator med i en RBL (Real-time Blackhole List) är den i grålistan 1000 sekunder. Automatisk vitlistning sker på sändande dator.
Riktiga e-postservrar som inte hanterar omsändningar förekommer, dessa kan vitlistas manuellt så att de inte drabbas av grålistning.

Grålistning fungerar på så sätt att om systemet inte sedan tidigare sett kombinationen ”avsändare-mottagare-avsändande nät (/24)”, så skickar KTH:s e-postsystem till den avsändande e-postservern ett temporärt fel och ber om att försöka skicka brevet senare. Detta för att stoppa spam-attacker.

Åtgärder

För att minska risken för att drabbas av spam attacker och minimera skadan krävs vissa åtgärder. Några exempel på dylika är:

- Blockering/filtrering/karantän av inkommande och utgående misstänkta brev med hjälp av spärrlistor - lokala eller publika
- Detektering och larm när en utgående spamattack utförs
- Fördröjning av sådan post genom s.k. "throttling"

- Detektering av och larm vid inkommande phishing liknande meddelanden
- Möjlighet att rensa användares e-postlådor från konstaterade spammeddelanden
- Möjlighet att snabbt detektera en spamattack via användares konto samt spärra kontot och rensa köer etc.

Antivirus

Med virus, "elakartad kod" avses programvara som innehåller för användaren okända funktioner som på något sätt är säkerhetsmässigt oönskade och som medvetet lagts in av tillverkaren. All central e-post genomsöks i syfte att finna virus, maskar, spionprogram och elakartad kod, i första hand kommer dessa att avlägsnas från meddelandet . Om detta misslyckas kommer brevet hamna i en s.k. karantän.

Beskrivning – virus/elakartad kod

Exempel på funktionalitet i ett virus/elakartad kod kan vara att logga alla tangentnedtryckningar som användaren gör (i syfte att fånga lösenord och annan känslig information), förstöra lagrad information eller att möjliggöra att datorn utnyttjas för utskick av skräppost eller annan typ av missbruk.

Motmedel – virus/elakartad kod

Det finns ett antal olika metoder och verktyg som man kan använda för att skydda sig mot elakartad kod. Det är dock viktigt att förstå, att det är endast en kombination av rätt verktyg och ett stort mått försiktighet som ger ett bra skydd. Man kan som vanlig datoranvändare, eller systemadministratör inte enbart förlita sig till datorns grundläggande säkerhetsfunktioner utan man måste kombinera antivirusprogram, antispionprogram, brandvägg och sund skepsis för att slippa problem. Tekniken skyddar oss inte, om vi inte dessutom är försiktiga när vi surfar på internet och i vårt dagliga datoranvändande. Ett bra sätt att skydda sig mot problem är att kombinera en brandvägg, ett antivirusprogram och ett antispionprogram med regelbunden uppdatering av operativsystemet och installerade program och ett stort mått av försiktighet och sunt förnuft. Inget av programmen är heltäckande, och olika tillverkare är olika snabba med att släppa virus/spywaredefinitioner. Alla som använder det centrala e-postsystemet ska ha en antivirusklient installerad oavsett operativ system.

Komponenter i e-postsystemet för att motverka virus

Viruskontroll i MX lagret: E-post som innehåller virus eller otillåtna filer sparas i karantän på respektive mx-server, samt skickas till en funktions e-postbox i Exchange. E-post med bifogade filer av typ: .exe, .com, .pif, scr ,.bat, m.fl. kastas automatiskt.

Viruskontroll på Exchange finns i 2 delar, dels på inkommande/utgående i e-posttransporten och dels på databasservrarna. I Exchange finns det tillgång till 5 st. olika antivirusmotorer för detektering av virus. Krypterade zipfiler och komprimerade filer hanteras som suspekta och sparas i karantän lokalt på servern. Korrupta komprimerade filer slängs vid detektering.

Phishinghantering

Phishing eller nätfiske går ut på att lura en annan person att avslöja hemliga uppgifter såsom t.ex. kontonummer, kreditkortsnummer lösenord etc. Det vanligaste är att man kontaktar offret via e-post eftersom detta är det billigaste och mest effektiva sättet att nå många. Breven är ofta utformade så att det ska se ut att komma från en bank eller någon IT-supportorganisation. Språket har tidigare varit dåligt, men detta har ändrat sig och utskicken är numera relativt välskrivna.

Effekter av phishing

När försöket lyckats och offret skickat iväg sina uppgifter kan flera olika saker inträffa. Det vanligaste när det gäller konto-/kreditkortsnummer är givetvis att man försöker föra över pengar eller betala med hjälp av den inkomna informationen. I fallet med skickande av konto/lösenord så är det vanligt att man använder aktuellt konto till att skicka ut stora mängder nya phishing meddelanden eller skräppost/spam. I samband med mera riktade attacker använder man kontoinformationen till att stjäla information eller hacka sig vidare.

Motmedel phishing via e-post

Det är inte helt enkelt att skydda sig mot denna typ av bedrägerier. Det viktigaste är som vanligt att informera användarna så att de aldrig skickar känslig information via e-post. Man kan upprätta olika spärrlistor med e-postadresser som man vet används i samband med phishingutskick, antingen egna eller publika som finns att ladda ner. Problemet med denna metod är att man ofta hinner få in ett stort antal meddelanden i systemet innan de aktuella adresserna dyker upp i spärrlistorna. När en adress hamnat i en spärrlista så kommer e-postsystemet inte längre att skicka e-post till eller från de spärrade adresserna, vilket innebär att fiskaren inte når sitt offer och den som försöker svara inte kan skicka ut information. Ett problem i sammanget är det faktum att man ofta inte har kontroll över en e-postanvändares utgående kommunikation - den kan t.ex. skötas från användarens hemmanätverk vilket inte sällan innebär att posten skickas via närmaste e-postserver hos aktuell ISP. Man kan således inte säkert veta vilka av användarna som svarat på phishing-försök.

Komponenter i e-postsystem för att motverka phishing

För att minska risken för att drabbas av phishingattacker och att användare svarar på dessa samt minimera skadan krävs vissa åtgärder. Några exempel på dylika är:

- Blockering/filtrering/karantän av inkommande och utgående phishing brev med hjälp av spärrlistor - lokala eller publika
- Detektering och larm när en användare svarar på phishingmeddelanden
- Detektering av och larm vid inkommande phishingliknande meddelanden
- Möjlighet att rensa användares e-postlådor från konstaterade suspekta meddelanden
- Möjlighet att snabbt detektera en spamattack via lurad användares konto samt spärra kontot och rensa köer etc. (Se även under SPAM) Virus/elakartad kod
- Systemadministratörer och användare vid KTH kan rapportera in misstänkt phishing i IRT-portalen, där listas även spärrade avsändaradresser

Användning av e-post på KTH

I det centrala e-postsystemet skapas med automatik e-postboxar till alla anställda och studenter på KTH. E-postboxarna skapas när kontot är genererat i den centrala användardatabasen UG.

E-post adresstyper

Personliga adresser

En personlig adress är direkt knuten till en unik person.

Gruppadresser/Distributionslista

En gruppadress går till alla medlemmar i en grupp.

Funktionsadresser

Funktionsadresser för e-post är adresser som riktar sig till en viss funktion istället för till en viss person. Funktionsadresser på KTH se bilaga 1.

Frånvarohantering

Alla anställda har ett ansvar att vid frånvaro hantera sin e-postbrevlåda. enligt något av följande alternativ:

- Aktivera e-postprogrammets frånvarohanterare. Ange under vilken tid frånvaron gäller, kontaktuppgifter till kollegor och/eller skolans registrator samt hänvisning till relevant funktionsbrevlåda.
- Aktivera automatisk vidarebefordran till en kollega eller skolans registrator.
- Dela ut sin e-postbrevlåda till en kollega.
- Att själv bevaka sin e-post

Om handlingar från en enskild e-postbrevlåda begärs ut och den anställde inte är anträffbar på grund av semester, sjukdom eller annan orsak åligger det KTH:s IT-administration att vidarebefordra e-post till KTH:s centrala registratur som då ska handlägga utlämnandet. Vidarebefordran till registraturen sker på anmodan av den som mottagit begäran om utlämnande. För KTH:s centrala e-postsystem ansvarar IT-supporten för vidarebefordran.

Förfaringssättet gäller även i andra situationer där tillgång till anställds e-post vid frånvaro krävs för att KTH som myndighet ska kunna fullgöra sina skyldigheter.

Signaturer

Gemensam signatur för KTH:s anställda finns framtagen för KTH.
Se referenser

E-postadresser

På KTH finns ett antal olika adresstyper som ska användas. Vilka adresser som är möjliga att använda och vilka regler vi följer. Funktionsadresser på KTH se bilaga 1.

Adressrymd

- Personliga e-postadresser består av 2-8 tecken a-z, 0-9. Adressen får inte börja med bokstaven "u" följt av en siffra.
- E-postadresser som består av fler än åtta tecken eller upp till åtta bokstäver (inga siffror) i kombination med minustecken '-' eller understrykningstecken '_' är reserverade för grupp- och funktionsadresser.
- Adresser på standardformat eller organisationsformat där mottagare motsvarar formatet på en kurskod, institutionskod eller likande är reserverade för gruppadresser.
- Adresser, oavsett format, där mottagare är ett vedertaget begrepp för en funktion, är reserverade för funktionsadresser.
- Undantag från ovanstående kan beviljas av e-postgruppen.

Otillåtna adresser

- Adresser på standardformat där mottagare består av förnamn kombinerat med efternamn är inte tillåtna
- Adresser, oavsett format, där mottagare innehåller andra tecken än bokstäverna 'a' till 'z', siffror samt punkt '.', minustecken '-' eller understrykningstecken '_' är inte tillåtna
- Adresser, oavsett format, där mottagare är ett ord som kan anses vara stötande eller har en politisk, religiös eller diskriminerande innebörd är otillåtna
- Adresser som sammanfaller med namn på vanligt förekommande systemkonton, system, reserverade ord i system, protokoll, tjänster, e-postalias, funktionsadresser samt adresser ii UG:s lista över förbjudna är inte tillåtna
- Adresser ska bestå av minst två tecken. Ifall synnerliga skäl föreligger kan undantag beviljas av e-postgruppen

- Undantag finns för vissa äldre adresser

E-postboxar

I det centrala e-postsystemet finns det generellt 3 olika sorters e-postboxar.

Personliga e-postboxar

En enskild individs brevlåda kopplad till en personlig adress.

Funktions e-postbox

En e-postbox som är opersonlig, dvs. en e-postbox som flera personer kan läsa och skicka som. Denna e-postbox är kopplad till en funktionsadress. Den kan läsas och besvaras av en eller flera personer. Fördelarna med funktionsadresser är bland andra:

- Flera personer kan bevaka och hantera posten till funktionen oberoende av semestrar, personalbyten m.m.
- Standardiserade funktionsadresser ger en naturlig och lättare hågkommen väg att kommunicera med myndighetsfunktionerna.
- Registrering och annan hantering av inkommande e-post underlättas vid användning av funktionsadresser.

Det är att föredra att e-post som adresseras till funktionskonton hanteras med hjälp av ett ärendehanteringssystem.

Funktionskalender

En opersonlig e-postbox vars funktion är att vara en kalender i det centrala e-postsystemet. Exempel på detta kan vara en bokningskalender för ett konferensrum eller en låneprojektor.

Kvota

Som standard har alla användare 2 GB utrymme i e-postsystemet. Ytterligare utrymme beviljas för anställda genom konsultation av IT- Supportcenter. Man får inte mer utrymme tilldelat om huvuddelen av utrymmet består av privat e-post. IT- Supportcenter har rätt att öka kvoten upp till 5 GB, över denna kvot kontaktas systemgruppen.

Avveckling av e-postboxar

E-postkontot finns kvar tills annat anges.

När man som personal slutar så kommer kontot att tas bort ur alla grupper för att sedan få affilieringen alumn.

Massutskick - anvisningar

Vid massutskick bör man fundera på vilka som är målgrupp och vilka som behöver läsa e-postmeddelandet. Det är inte alltid som samtliga mottagare anser att informationen är relevant/intressant. Är innehållet i ett eventuellt bifogat dokument verkligen av intresse för läsaren, eller kan det förmedlas på ett snabbare och enklare sätt i brevtexten? Därför gäller följande för utskick till fler än 20 mottagare.

- Syfte, målgrupp och adresskälla ska tydligt framgå i brevet
- Massbrev i marknadsföringssyfte eller reklamsyfte är inte tillåtet, inte ens för ideell verksamhet

- Det är inte tillåtet att skicka e-post som innehåller politisk, religiös, rasistisk eller sexistisk propaganda
- Språket i brevet ska hållas på en nivå så att det inte uppfattas som oseriöst.
- En enskild mottagare ska inte kunna se vilka övriga e-postadresser brevet har skickats till.
- Avsändare ska vara adress@kth.se
- Vid eventuella tveksamheter eller frågor, kontakta postmaster@kth.se innan utskicket görs. Ifall utskicket bedöms som legitimt så får avsändaren en signatur att bifoga utskicket där det framgår att innehållet har granskats och godkänts av postmaster

Skriv ”för kännedom” om mottagaren inte förväntas agera på e-postmeddelandet. Alternativt kan en kopia på e-postmeddelandet skickas, vilket signalerar att meddelandet skickat för kännedom.

KTH:s intranät ska användas till större målgrupper. Tänk på att intranätet passar bättre för många allmänna typer av meddelanden, kallelser, protokoll etc. där målgruppen är en hel arbetsgrupp, avdelning eller förvaltning.

Skicka inte lustigheter, kedjebrev, tiggarbrev med mera i tjänsten oavsett hur behjärtansvärt ändamålet kan upplevas.

Utskick till många mottagare på kort tid kommer automatiskt att larmas till IRT. Vitlistning är möjligt och görs enligt fastställd rutin – att göra massutskick på KTH.

Hur gör man massutskick?

För att stora utskick inte ska fastna i spamkarantän ska man först kontakta IT-SupportCenter, då kommer din adress att vitlistas vid utskickstillfället. Du skickar ett e-postmeddelande till it-sc@kth.se, i meddelandet beskriver du vilken adress du ska skicka ifrån och när det ska göras.

Skräppost/Junk e-post

Allt som finns i mappen skräppost (Skräppost/Junk) är att betrakta som icke gallrat dvs. fortfarande en allmän handlig, autotömning sker efter 365 dagar .

Papperskorg

Allt som finns i papperskorgen (Deleted Items/Trash) är att betrakta som icke gallrat dvs. fortfarande en allmän handlig, autotömning sker efter 365 dagar .

Adressböcker

Alla anställa och studenter finns i globala adressboken, denna har alla som har central e-postbox tillgång till. I LDAP syns anställdas telefonnummer och adress till arbetsplatsen. Detta är godkänt för publicering då du skrivit på ansvarsförbindelsen.

Åtkomst till det centrala e-post systemet

Det finns ett antal olika sätt att nå din e-postbox i det centrala e-postsystemet:

- IMAP
- MAPI för Outlook
- Outlook anywhere (RPC över https). Teknik att köra Outlook utanför KTH: s nät utan att behöva köra vpn (stödjs av Outlook 2003 och senare).
- POP 3
- Webmail
- Webservices (för bl.a. entourage och mail på mac)

- Kalender
- Autokonfiguration för klienter (Outlook 2007 och senare)
- Exchange active-sync för mobiler/smartphones

Hur man konfigurerar sin klient får man information om från IT-SupportCenter.

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

Personlig integritet i e-postsammanhang

Ansvarsförbindelsen reglerar vad som är tillåtet för IT-personal att göra med innehållet i

e-postboxen.

PUL

När man skrivit på ansvarsförbindelsen innebär det att ens personuppgifter kommer att förekomma i KTH:s system.

Alumni

Alumni får inneha e-postkonto.
Se referenser.

IT-avdelningens rutiner när anställd avlider

Systemgruppens åtgärder

Inaktivera datorkonto

Ta bort namn från adresslistan i Exchange/LDAP

- Studsa e-post i mx
- Ta bort e-postbox
- Arkivera e-postbox till hemkatalog

Begrepp

Alias – Ett alternativt namn på en användare eller en e-postadress.
Användare – En unik person som har tillgång till en eller flera av KTH: s datorresurser.
KTH-konto – En unik identifierare av en användare.
Postmaster – En funktion har ansvar för att informera, planera, upprätthålla och utveckla e-postsystemet/diskyta. Administrerar e-postserver och kringliggande system.
Quota – En enskild användares tilldelade utrymme för e-post.
Skräppost/junk e-post/spam – Oönskad e-post.
Papperskorg/deleted items – Utrymme för raderad e-post.
Funktionsadress – En e-postadress som går till en viss funktion t.ex. registrator@kth.se
RFC – Request For Comments är ett dokument som beskriver en standard.
Se vidare: för ytterligare information om RFC: http://www.ietf.org/rfc.html

Alumn - Före detta anställd eller student
Standardformat – E-postadresser på standardformat: mottagare@kth.se
Organisationsformat - E-postadresser på organisationsformat: mottagare@organisation.kth.se
Dessa adresser är knutna till och/eller delegerade till en organisation på KTH.

Kompletterande anvisningar

Frågor besvaras av: postmaster@kth.se

Vidarebefordran

För att kunna garantera efterlevnad av KTH:s myndighetskrav så är automatisk vidarebefordran till externt e-postsystem (ex. Google, Hotmail osv.) inte tillåten. Anledningen till detta är att kunna säkerställa att den kommunikations som är av offentlig karaktär inte förloras. Den skall kunna spåras, följas upp och i ett ev. senare skede omprövas. Ett exempel är kommunikation mellan lärare och student.

Dock kan det finnas särskilda skäl att vidarebefordra sin e-post till annat system, även externt. Det medges genom att man skickar in en formell beställning till IT-Support Center (alternativt sin lokala IT-support), denna skall vara undertecknad av närmaste chef. Blanketten hittas hos IT-Support Center. Denna formalia syftar främst till att belysa ansvarsdelen och tydliggöra vikten av spårbarhet, osv.

Intern vidarebefordran som görs till ex. csc, nordita osv. får naturligtvis göras, under förutsättning att e-post systemet hos den mottagande skolan/enheten har rutiner som följer och lever upp till de krav som krävs enligt denna föreskrift.

Massutskick

De s.k. massutskicken i KTH:s e-post system kommer from den 1 november 2011 att hanteras av avdelningen för kommunikation och internationella relationer på KTH. De kommer att ansvara för reglerna, rutinerna och det operativa arbete som innefattas av detta. Syftet är att effektivisera utskicken och undvika onödig e-post.

E-postgruppen

Detta är arbetsgruppen som hanterar e-postfrågor för KTH:s centrala e-postsystem. E-postgruppen utses av och arbetar på delegation av IT-ledningsgruppen. Gruppens uppdrag och sammansättning presenteras nedan.

Arbetsgruppen:

- Ska bestå av minst två representanter från centrala IT-avdelningens drift- och supportorganisation
- Representanter från minst två skolor ska finnas, som tillför dess perspektiv på frågorna
- Kompetensen i gruppen har tyngden på det tekniska med stort säkerhets, drift och kundfokus
- Gruppen har befogenhet att fatta beslut i de dagliga tekniska frågorna