GÖTEBORGS UNIVERSITET

Feb 2015

1 Regler för användning av Göteborgs universitets IT- resurser

1.1 Allmänt

Göteborgs universitets (GU:s) IT-resurser ägs av universitetet och är avsedda att användas i och för universitetets verksamhet att tillhandahålla utbildning, forskning och därtill knuten administration samt för samverkan med det omgivande samhället. Resurserna får inte tas i anspråk för ändamål genom vilka universitetets namn, anseende och goda rykte kan skadas.

Med IT-resurser avses datorer, mobiltelefoner, surfplattor, programvaror, programvarulicenser, kommunikationsnät och all annan kringutrustning som nyttjas i samband med kommunikation och hantering av information i digital form.

1.2 Regler för användning

1.2.1 Begränsningar i nyttjandet av universitetets IT-resurser

Universitetets IT-resurser får inte nyttjas för att på otillbörligt eller oetiskt sätt sprida, förvara eller förmedla information

- i strid mot gällande lagstiftning, t ex hets mot folkgrupp, barnpornografibrott, olaga våldskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott
- som, utan koppling till användares roll vid GU, är att betrakta som politisk, ideologisk eller religiös propaganda
- i strid mot personuppgiftslagens stadganden om den personliga integriteten
- som är personligt kränkande eller stötande
- som syftar till att marknadsföra produkter eller tjänster som saknar anknytning till universitetet
- i strid mot av GU ingångna avtal avseende IT-resurser
- eller på annat sätt störa GU:s IT-verksamhet

Universitetets IT-resurser får endast i begränsad omfattning användas för privat bruk.

1.2.2 Ansvar och befogenheter

Innan användare ges behörighet att nyttja GU:s IT-resurser skall han/hon informeras om gällande regler för användning och underteckna ”Ansvarsförbindelse för användning av GU:s IT-resurser” eller på annat sätt bekräfta att han/hon tagit del av reglerna t.ex. via ett godkännandeformulär i medarbetarportalen.

Användaridentiteten skall alltid kunna spåras därför är det inte tillåtet att använda någon annans behörighet eller utnyttja felaktiga konfigurationer, programfel eller på annat sätt manipulera IT-resurserna.

Den tilldelade behörigheten är tidsbegränsad och är kopplad till studier, anställning, projektdeltagande eller uppdrag. Användaren skall själv meddela omständigheter som medför att behörigheten skall upphöra.

1.3 Regler för användning av Internet och e-post

1.3.1 Allmänt

GUNET/SUNET är snabba nät och en dator ansluten till dessa är därför ständigt utsatt för intrångsförsök. Information som sänds eller görs åtkomlig via Internet kan även bli åtkomlig för obehöriga. Varje användare har ett ansvar att skydda GU:s IT-resurser mot intrång och information mot åtkomst för obehöriga.

Därför skall

- datorer och datorsystem alltid vara skyddade med säkert konstruerat lösenord, se punkt 1.5, eller annan teknisk behörighets- och användaridentifikation
- datorer som ägs/hyrs av GU ha av GU licensierade antivirusprogram och andra av GU rekommenderade skyddssystem. Definitionerna skall vara uppdaterade.
- övriga datorer som ansluts till GU:s IT-resurser ha likvärdigt skyddssystem installerat för att uppnå ett tillräckligt skydd. Definitionerna skall vara uppdaterade.
- alla dokument/filer virustestas innan de öppnas eller laddas ner på användarens dator
- användaren aldrig ladda ner program och filer till en dator som är ansluten till GU:s IT-resurser utan att analysera säkerhetsrisken
- alla intrångsförsök anmälas till universitetets IT-support eller studentsupport
- konfidentiell information som skickas med e-post eller görs åtkomlig via Internet skyddas utifrån resultatet av genomförd informationsklassning

Vid osäkerhet om ovanstående reglers tillämpning skall IT-support eller studentsupport kontaktas.

1.3.2 Användning av Internet

Det är förbjudet att nyttja GU:s IT-resurser för att ladda ner upphovsrättsskyddat material utan rättighetsinnehavarens tillstånd.

När man publicerar sig på GU:s webb skall GU:s regler ” Regler för publicering på Göteborgs universitets webbplatser” följas. Vid tveksamhet om publicering av personuppgifter skall kontakt tas med GU:s personuppgiftsombud före publicering.

Den medarbetare som inom ramen för sin anställning använder sig utav socialt media eller molntjänst skall, innan användningen, ta ställning till de risker i förhållande informationen/materialet, som kan kopplas till användning av mediet och tjänsten. Det avser t.ex. upphovsrätt, personlig integritet och innehållet i användarförbindelsen eller annat avtal. Riskbedömningen görs utifrån GU:s regler för informationsklassning.

1.3.3 E-post

All e-post som skickas från en adress inom GU representerar universitetet. I e-post skall det finnas korrekta uppgifter om avsändarens namn och adress.

Innan man skickar e-post meddelanden skall adressen kontrolleras noga, så att brevet når till rätt adressat.

1.3.4 E-post som hanteras av GU:s medarbetare

E-post omfattas av reglerna för allmänna handlingar. Registrering (diarieföring) av allmänna handlingar, i form av e-post, skall därför ske enligt samma regler som vanliga pappersdokument.

Varje medarbetare har ansvar för att hantera inkommande e-post samt att vid frånvaro se till att den tas emot och vid behov handläggs.

All mottagning och sändning av e-post till/från GU skall ske med hjälp av GU:s e-postservrar. Om man behöver hantera e-post för universitetet när man inte är direkt kopplad till GU:s IT-resurser, skall man skaffa sig tillgång till en av GU:s egna webbtjänster eller annan, av tekniskt ansvarig godkänd, anslutning för detta.

Det är inte tillåtet att automatiskt vidaresända e-post riktad till en GU-adress till en extern adress. E-post ställd till GU skall också besvaras av en GU-adress.

1.4 Regler för medarbetares distansåtkomst mot GU:s IT-resurser

1.4.1 Allmänt

För att upprätthålla god säkerhet vid distansåtkomst ställs det krav på hög säkerhet i hela kommunikationskedjan från användare, utrustning och program fram till nyttjad IT-tjänst.

För åtkomst av viss IT-tjänst skall användaren själv ta reda på vilka regler och anvisningar som informationsägare och/eller systemägare och IT-leveransägare satt upp för den aktuella IT-tjänsten och ingående IT-system.

1.4.2 Distansåtkomst från privat dator

I syfte att upprätthålla god säkerhet även vid arbete från privat datorutrustning mot någon av GU:s IT-resurser skall denna ha minst motsvarande skydd som av GU ägda/-hyrda datorer. Den privata datorutrustningen skall ha

- individuella lösenord, se pkt 1.5 nedan
- uppdaterat antivirusprogram
- säkerhetsmässigt uppdaterade programvaror
- av GU godkänd anslutning

Vid bredbandsuppkoppling skall ett extra intrångsskydd genom en så kallad brandvägg vara installerat.

1.5 Regler för lösenord och inloggning

Universitetets IT-system respektive varje användare, skall skyddas med lösenord och/eller annan teknisk behörighets- och användaridentifikation.

För att skyddet genom lösenord skall fungera effektivt skall följande kriterier vara uppfyllda.

- Användaridentitet, lösenord och tilldelad behörighet skall vara personlig.
- Lösenorden skall hållas hemliga och får inte lånas ut.
- Ett lösenord skall vara konstruerat med minst 8 tecken som är blandade med versaler, gemener, siffror och något specialtecken. Det får inte anknyta till den egna personen

såsom namn, födelsedatum, utgöra enkla ord eller dylikt och inte heller bestå av tangenter som sitter i grupp.

- Lösenordet skall bytas var 6:e månad eller så fort det blir känt för någon utomstående.
- Funktionen för automatisk skärmlåsning (energisparläge) efter max 10 min inaktivitet skall alltid vara inkopplad. För fortsatt arbete på datorn måste den alltså låsas upp med ett lösenord.
- Användaren skall alltid logga ut från datorn när den lämnas utan egen uppsikt.

1.6 Påföljder och åtgärder vid regelbrott

Överträdelse av dessa regler kan medföra att användare helt eller delvis stängs av från nyttjande av universitetets IT-resurser. Beslut tas av verksamhetsansvarig för det aktuella ansvarsområdet.

Tekniskt ansvarig kan, i den akuta situationen, med omedelbar verkan stänga av misskött eller missbrukad IT-resurs.

Överträdelse av dessa regler anmäls av prefekt/motsvarande till

- rektor beträffande studenter. Rektor har att ta ställning till om ärendet skall hänskjutas till disciplinnämnd. De disciplinära påföljderna är varning eller avstängning under viss tid från undervisningen och annan verksamhet vid universitetet
- personalansvarsnämnd beträffande anställd. Påföljden kan bli disciplinansvar eller avstängning.

Misstanke om brott kan medföra polisanmälan.