



ANVISNINGAR OM INFORMATIONSSÄKERHET FÖR STUDERANDE

Augusti 2010

INNEHÅLL

Varför är informationssäkerhet och dataskydd viktigt?	1
Nyttjanderätt och bra lösenord	2
Hur man använder nätet och e-posten förnuftigt	3
Dataskydd och sekretess.....	5
Kom i håg när du använder universitetets datorer.....	6
Hur du använder och underhåller din egen dator.....	8
Hur du använder allmänna datorer och publika trådlösa nät.....	9
Media och säkerhetskopior	10
Upphovsrätt och programlicenser	11
Då studierätten upphör	12
När din dator infekteras och säkerhetsincidenter	13
Tilläggsinformation och länkar	bakpärmen

Denna anvisning är i första hand avsedd för universitetsstuderande. Den är gjord som ett samarbetsprojekt mellan universiteten och vi har strävat till att den skall lämpa sig för alla universitet. Vi tackar ledningsgruppen för informationssäkerhet inom statsförvaltningen (VAHTI), som har producerat Informationssäkerhetsanvisningar för personalen (VAHTI 7/2008) och den har vi haft som en förebild för denna anvisning. Vi vill också tacka universitetens gemensamma sec-arbetsgrupp för informationssäkerhet för kommentarer.

Arbetsgrupp: Kenneth Kahri (Helsingfors universitet), Olavi Manninen (Kuopion yliopisto) och Kaisu Rahko (Oulun yliopisto)

Svensk bearbetning: Ulf Pensar (Hanken), Matti Huvila (Åbo Akademi) och Urpo Kaila (CSC – Tieteen Tietotekniikan Keskus Oy)

Ombrytning och bilder: Katja Koppinen och Raija Törrönen (Kuopion yliopisto)

Anvisningen har gjorts på tjänstens vägnar och den är licensierad enligt Creative Commons Erkännande-Icke kommersiell-Dela lika: http://www.creativecommons.se/?page_id=193

VARFÖR ÄR INFORMATIONSSÄKERHET OCH DATASKYDD VIKTIGT?

- Datorerna och nätet är viktiga redskap vid studierna och på fritiden. När du använder nätet utsätter du dig för olika risker. För att undvika dessa risker bör du veta något om informationssäkerhet samt om dataskydd.
- Informationssäkerheten omfattar allt som gör att tjänster och system fungerar korrekt, är pålitliga och säkra att använda.
- Dataskydd (eller datasekretess) betyder att man skyddar människans privatliv och integritet när man hanterar personuppgifter.
- För att skydda privatlivet är det viktigt att du uppmärksammar kraven på dataskydd när du använder IT-tjänster. Skydda både uppgifter om dig själv och personuppgifter om andra, som du har tillgång till. Alla har någonting som bör skyddas, t.ex. person-, kontakt-, bank- och hälsouppgifter, e-postmeddelanden eller foton.
- Informationssäkerheten anses ofta vara svårbegriplig men genom att använda sunt förnuft och följa anvisningar klarar du av att lösa de flesta problemen.
- Alla bör ta ansvar för informationssäkerheten. Universitetets informationssäkerhetspolicy slår fast bland annat att studerandena bör följa anvisningarna för att skydda sig själv och för att skydda andra. En säkerhetsincident kan få rättsliga påföljder.
- Om du vid sidan av studierna innehar förtroendeuppdrag är ditt ansvar större än för en vanlig studerande. Ta reda på vad detta ansvar medför.

NYTTJANDERÄTT OCH BRA LÖSEWORD

- Rätten att använda universitetets datasystem är personlig och får inte överlåtas åt en annan person.
- Vanligen loggar man in till universitetets datorer och system med användarnamn (eller användar-ID) och lösenord. Behandla ditt användarnamn och ditt lösenord med samma omsorg som ditt bankkort och din pinkod.
- Vid vissa universitet kan man använda smartkort (t.ex. studerandekort eller Lyyra-kort) vid autentisering till IT-system samt vid passerkontroll och för att öppna dörrar. Var omsorgsfull med ditt smartkort, låna inte ut kortet åt andra, eftersom innehavaren ansvarar för hur kortet används.
- Du ansvarar för det som utförs med ditt användarnamn. Ge inte ut ditt användarnamn, lösenord eller ditt smartkort åt någon annan. Inte ens systemadministratören bör känna till ditt lösenord. Om någon frågar efter ditt användarnamn och ditt lösenord är han/hon ute i skumma ärenden.
- E-post- och andra tjänster som universitetet erbjuder dig är i första hand till för dina studier. Du kan också använda dessa tjänster för privat bruk i måttlig grad så länge det inte stör andra.
- Allmänt taget är kommersiellt bruk av universitetets system förbjudet. Det är också förbjudet att använda systemen till icke-universitetsrelaterad politisk verksamhet såsom valreklam.
- Ett bra lösenord kommer du lätt ihåg men det är svårt för utomstående att gissa sig till. Undvik att skriva upp ditt lösenord.
- Använd varken lösenord som kan förknippas med dig eller vanliga ord. Välj ett lösenord som innehåller små och stora

bokstäver, siffror och/eller specialtecken. Specialtecknen fungerar inte i alla system, kontrollera detta med universitetets anvisningar.

- Om du har fått ett nytt lösenord från universitetets IT-stöd skall du genast byta det till ett lösenord som bara du känner till.
- Byt lösenorden tillräckligt ofta i enlighet med universitetets anvisningar och omedelbart om du misstänker att någon annan fått tag i det. Lösenordet som du använder vid universitetets tjänster får inte användas vid utomstående tjänster.

HUR MAN ANVÄNDER NÄTET OCH E-POSTEN FÖRNUFTIGT

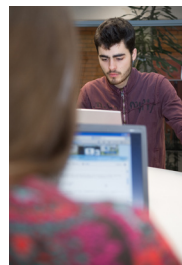
- Vanligen sänder man information via internet i okrypterad form utan något skydd. Du bör därför vara försiktig när du använder e-posten och nätet.
- Universitetet ger varje studerande ett användarnamn och en e-postadress. I första hand bör du använda denna e-postadress för universitetets tjänster och system, bl.a. i studentregistret och i inlärningsmiljöer (Oodi, Optima, Moodle, Blackboard osv.)
- Bekanta dig med nätetiketten och följ den när du använder epost och vid annan kommunikation. Det är oartigt att skriva alltför hätskt på t.ex. diskussionsforum. Kränkande nätskriverier har lett till fällande domar.
- Epostbilagor kan innehålla sabotageprogram dvs. skadlig kod. Var på din vakt inför suspekta epostmeddelanden och speciellt bilagor. Öppna inte suspekta meddelanden. Vid behov kan du be om råd av IT-stödet.

-
- Reklam och kedjebrev som skickats utan mottagarens tillstånd är skräppost. Du ska inte svara eller skicka dessa meddelanden vidare utan radera dem omedelbart. Skräppostmeddelandena kan innehålla sabotageprogram eller länka användaren vidare till en sida som innehåller sabotageprogram.
 - Universiteten använder sig av olika metoder för att filtrera bort skräpposten. I vissa system är filtreringen automatiskt påslagen och i vissa system bör användaren själv aktivera blockeringen. Ta själv reda på vad som gäller för ditt universitet.
 - Inta en skeptisk inställning till hur trovärdigt ett meddelande är. Ett epostmeddelande kan också vara skickat av någon annan än den avsändare som anges i adressfältet. Virus kan också skicka ut epost utan att användaren behöver göra någonting alls.
 - Var speciellt uppmärksam på s.k. nätfiske där du uppmanas att uppge ditt användarnamn och ditt lösenord eller dina bankuppgifter under någon förevändning som kan låta saklig.
 - Om du får epost avsedd för någon annan, meddela avsändaren om detta. Kom ihåg att du har tystnadsplikt angående epostmeddelande avsedda för andra.
 - Kontrollera att du har korrekta epostadresser och att inga skrivfel finns i dessa innan du skickar iväg meddelandet.
 - Överväg till vem eller var du publicerar din epostadress. Skaffa dig en gratisadress (t.ex. Hotmail, Gmail) och undvik att använda universitets adress på allmänna nätforum (t.ex. Facebook, MySpace).
 - Använd endast kända och pålitliga nättjänster.

-
- Välj en epostservice som krypterar trafiken (i webbposten ser du https:// i adressfältet. Dessutom ser du en låst låsikon i adressfältet eller i webbläsarens nedre hörn) om du använder annan postservice än universitetets epost.
 - Använd inte nättjänster under ett användarnamn som har administratörrättigheter (Administrator, root)

DATASKYDD OCH SEKRETESS

- Tänk efter hur du hanterar personuppgifter och åt vem du kan överlåta dem.
- Du kan själv bestämma åt vem du överlåter dina egna personuppgifter, men om du ska överlåta en annan persons uppgifter måste du ha tillstånd eller annan befogenhet.
- Tänk också efter hur du lägger ut uppgifter om dig själv och om andra i sociala nätverk som Facebook, Myspace eller motsvarande webbtjänster. Det kan vara omöjligt att efteråt få bort personuppgifter som ett foto eller en hemadress från nätet efteråt.
- I sociala nätverk är det lätt att låtsas vara en annan eller en annorlunda person. Var inte alltför lättlurad utan förhåll dig med en viss skepsis till allt.
- Kom ihåg att andra kan höra dig och känna igen dig när du talar i mobiltelefon på allmän plats. Tala inte om känsliga eller konfidentiella saker så att obehöriga hör dig.



KOM I HÅG NÄR DU ANVÄNDER UNIVERSITETS DATORER

- Se till att obehöriga inte tittar på din skärm eller ditt tangentbord när du loggar in och när du hanterar annan känslig information.
- Logga alltid in bara med ditt eget användarnamn. Kom ihåg att logga ut när du slutar och innan det, städa efter dig:
 - Töm webbläsarens temporära filer, webbhistorik och cookies som kan ha sparats från din session.
 - Radera också andra temporära filer som du kan ha lämnat efter dig på datorn.
 - Kom också ihåg att ta med dig din minnesticka och dina papper.
- Om du temporärt lämnar datorn, ta med dig din minnespinne och annat material.



Lås Windows (Win+L).

- Lås datorn så att andra inte kan använda ditt användarnamn eller se dina filer.
- Lås Windows datorn genom att trycka på (Win+L).
- Kom ihåg att det kan vara förbjudet att låsa datorn för en längre tid för då kan inte andra använda den.

-
- Spara din text och dina filer som är viktiga för dig i din hemkatalog på universitets filserver. Universitet sköter säkerhetskopieringen av dina filer.
 - Kom ihåg att med jämna mellanrum spara din text eller dina andra filer, speciellt om du arbetar en längre tid med samma fil. Då förlorar du inte vad du har skrivit vid ett tekniskt fel.
 - Ta reda på var printern befinner sig innan du printar på en gemensam printer. Hämta din utskrift utan dröjsmål och kom ihåg att låsa datorn när du går efter utskriften.
 - Universitetets datorer är i första hand avsedda för studier och för arbetsuppgifter. Använd inte universitets datorer för privata ändamål om det finns andra som köar för att få använda datorn.
 - Ofta har datacentralen förbjudit användarna att installera program på universitets datorer. Ibland kan detta också vara spärrat på teknisk väg. Om du behöver något speciellt program ta kontakt med IT-stödet. Det är möjligt att programmet kanske redan finns färdigt installerat på en annan dator eller möjligen kan det anskaffas av datacentralen.
 - Om du har fått en nyckel eller ett passagekort till en låst datorsal stäng dörren efter dig och släpp inte in obehöriga till salen.

HUR DU ANVÄNDER OCH UNDERHÅLLER DIN EGEN DATOR

- Universitetet sköter om informationssäkerheten för universitetets datorer. Om du har en egen dator, bör du själv sköta om att den är säker och uppdaterad.
- Sköt om din dator enligt god administrationspraxis.
- God administrationspraxis förutsätter att det finns uppdaterade brandväggs och antivirusprogram på datorn, att operativsystemet och också andra program uppdateras automatiskt (t.ex. med Windows Update)
- Använd administrativa konton – (t.ex. Administrator, root) endast för systemadministration, för att installera program eller för att skapa nya användarnamn.
- För normalt bruk skall du skapa ett vanligt användarnamn åt dig själv utan administrationsrättigheter. På detta sätt kan du skydda dina personuppgifter och minska risken för att drabbas av skadlig kod.
- Installera endast sådana program som du behöver. Onödiga program kan öka risken för att drabbas av sabotageprogram. Installera endast program som kommer från väl kända källor.
- Ta regelbundet säkerhetskopior på dina viktiga filer.
- Tänk efter vad som går förlorat om din hårddiska plötsligt får ett fel eller om din dator smittas av ett sabotageprogram.
- Var omsorgsfull när du transporterar eller lägger undan en bärbar dator. Skydda datorn mot stötar, damm och fukt. Lämna inte datorn i en bil eller göm den åtminstone i så fall.

-
- Om du har ett eget trådlöst nät, aktivera nätets säkerhetsinställningar (välj t.ex. WPA2) för att inte obehöriga ska kunna missbruka din uppkoppling eller följa med vad du själv gör i nätet. Följ nätapparaternas bruksanvisningar.
 - Om du har en egen bredbandsuppkoppling kontrollera i bruksanvisningen om det finns en brandvägg inbyggt. Om möjligt ta den i bruk.
 - Följ regelbundet med varningar om sårbarheter i datorprogram (t.ex. via <http://www.cert.fi/> och <http://www.sitic.se/>).

HUR DU ANVÄNDER ALLMÄNNA DATORER OCH PUBLIKA TRÅDLÖSA NÄT

- Allmänna datorer på nätcaféer kan vara behändiga när du vill läsa din epost eller när du vill logga in på sociala nätverk medan du är på resa. Du ska ändå inte lita på att de allmänna datorerna är säkra eller att det inte finns virus eller annan skadlig kod i dem.
- Tänk efter på förhand vad du vill göra och om är det nödvändigt att du använder ditt eget användarnamn för att logga in. Tänk också efter vilken typ av information du hanterar med den främmande datorn.
- Du lämnar nästan alltid spår efter dig när du använder dator och program: webbhistorik, temporära filer, cookies, sessionsdata, logfiler och andra spår av vad du har gjort. Ta på förhand reda på hur du själv kan radera dessa spår, t.ex. genom att radera besökta sidor och temporära filer i webbläsaren.
- När du använder trådlösa nät, kontrollera om din nätförbindelse är krypterad. Publika trådlösa nät t.ex. på caféer eller flygterminaler baserar sig ofta på okrypterade förbin-

delser och då kan andra avläsa din trafik. Då skall du helst använda bara sådana tjänster där applikationen själv sköter om krypteringen. I din webbläsare kan du se detta genom att det dyker upp en bild på ett låst lås i läsarens nedre (eller övre) hörn och webbadressen börjar på <https://>.

MEDIA OCH SÄKERHETSKOPIOR

- Universitetet säkerhetskopierar dina filer, om du lagrar dem i din hemkatalog på filservern.
- Minnesstickor är behändiga för att kopiera data och för säkerhetskopiering – använd dem ändå inte som det primära eller det enda mediet. En minnespinne försvinner lätt – lagra därför inte känsligt material på stickan.
- Var försiktig med andras minnesstickor. Det kan finnas sabotageprogram på dem. Programmet kan startas automatiskt då stickan kopplas till datorn, och då smittas din dator också.
- Om du hittar en främmande minnespinne på universitetet, ge den till universitetets ITstöd utan att undersöka dess innehåll.
- Om du har en egen dator, ta regelbundet säkerhetskopior av dina filer. Lämpliga media för säkerhetskopiering är bl.a. externa USB-skivorskivor, minnesstickor samt DVD- eller CD-skivor. Märk säkerhetskopiorna (innehållet och tidpunkten). Testa regelbundet kopiornas läsbarhet.
- Förvara säkerhetskopiorna skilt från datorn och i mån av möjligheter på ett låst ställe.
- Lär dig att hålla ordning på ditt material både i datorn, på minnesmedia och på dina papper. Då är det lättare för dig att skydda din information.

-
- Kasserade hårdskivor, minnesstickor och andra minnesmedia samt pappersmaterial som innehåller konfidentiell information ska inte kastas i soporna. Materialet ska förstöras på ett adekvat sätt: data som finns på minnesstickor, hårdskivor och andra elektroniska media förstörs genom överskrivning eller genom att krossa mediet. Pappersmaterialet förstör du genom att skära det i strimlor.

UPPHOVSRÄTT OCH PROGRAMLICENSER

- Installera endast sådan mjukvara i din dator som kommer från säkra källor och du har nyttjanderätt och licens till eller som är gratis. Installera inte olagliga kopior eller programvara, vars användningsrätt du är osäker på.
- Via ditt universitet kan du få licenser till vissa program, noggrannare information om detta hittar du i universitetets anvisningar.
- Kom ihåg att nyttjanderätten till program ofta har begränsats till studierna. Din rätt att använda dem upphör samtidigt som din studierätt upphör. Då nyttjanderätten upphör skall du avlägsna programmen från alla datorer, där du installerat dem.
- Användningsvillkoren för bibliotekens elektroniska material begränsar vem som får använda materialet och för vilket ändamål materialet får användas. Ta reda på dessa villkor genom att bekanta dig med bibliotekens och materialtjänstens anvisningar.
- Upphovsrätten skyddar filmer och musikmaterial. Kopiera inte dem från nätet och distribuera dem inte till nätet utan upphovsmannens särskilda tillstånd. Nuvarande lag om upphovsrätt tillåter inte utan tillstånd kopiering av datorprogram för enskilt bruk och stipulerar straff för olovlig distribution.

-
- Citera text i dina övningsarbeten och avhandlingar endast i den omfattning som rätten att citera tillåter. När du citerar, berätta vad och vem du citerade. Ta alltid reda på rätten att använda material innan du citerar det eller länkar det till ditt eget material.

DÅ STUDIERÄTTEN UPPHÖR

- Rätten att använda universitets IT-tjänster är bunden till din studierätt.
- Då du blir färdig med studierna eller din studierätt upphör, upphör också rätten att använda tjänsterna och ditt användarnamn inaktiveras, oftast automatiskt. Efter en viss tid raderas ditt användarnamn, e-posten och andra filer. Du ska beakta följande innan användarnamnet stängs:
 - Informera dina vänner andra kontakter om att e-postadressen ändras.
 - Kopiera de filer som du vill spara från universitetets servrar och radera resten.
 - Kopiera din e-post eller skicka den vidare till din nya e-postadress.
 - Avinstallera de program som du fått av universitetet och som du inte längre har rätt att använda i din dator.

VAD GÖRA NÄR DIN DATOR INFEKTERAS OCH VID SÄKERHETSINCIDENTER

- Om du misstänker att det finns eller har funnits ett sabotageprogram på en dator som du använder, gör på följande sätt:
 1. Byt genast via en annan dator alla lösenord som du har använt på datorn i fråga.
 2. Också liknande lösenord utgör en risk. Om du har använt din nätbank, kontakta banken och berätta om incidenten.
 3. Om datorn är din egen, sluta omedelbart att använda den och ta reda på hur du blir av med sabotageprogrammet. Om datorn ägs av någon annan, kontakta ITstödet och berätta om dina misstankar.
- Du kan få hjälp med att rensa din dator av universitets ITstöd, men läs först universitets anvisningar om virusbekämpning. Företag som producerar antivirusprogram har webbsidor som ger råd om hur man söker och avlägsnar sabotageprogram.
- Om du har skäl att misstänka att det föreligger en kränkning av datasekretessen, en säkerhetsincident eller missbruk av systemet, kontakta systemansvariga eller IT-stödet. Om det gäller ditt eget universitet, kontakta IT-stödet, annars ring växeln och be om att kopla till den person som ansvarar för informationssäkerheten. Berätta tydligt vad du har observerat och när detta hände. Uppge också ditt namn och dina kontaktuppgifter för eventuellt behov av tilläggsinformation.

TILLÄGGSINFORMATION OCH LÄNKAR

- Sidor om informationssäkerheten vid ditt universitet
 - » <http://www.hanken.fi/student/datasakerhet>

- Bekantadigmedsäkerhetsanvisningar för ditteget universitet
 - Anvisningar för säker nätanvändning
 - » www.tietoturvaopas.fi/sv
 - » www.tietoturvakoulu.fi/sv

 - Anvisningar för behandling av personuppgifter och integritetsskydd
 - » www.tietosuoja.fi/1559.htm

 - Nätetikett: God sed vid nätkommunikation
 - » sv.wikipedia.org/wiki/Netikett

 - Anvisningar för skydd av kommunikation, meddelanden om hot mot informationssäkerheten
 - » www.cert.fi/sv

 - Anvisningar för användning av mobiltelefoner
 - » www.ficora.fi/mobiiliturva/svenska

 - Statens författningsdata
 - » <http://www.finlex.fi/sv>

 - Helsingfors universitets IKT-körkort
 - » <http://apumatti.helsinki.fi/lcms.php?am=18337-18337-1&page=19813>