Stockholms universitet

2018-05-25

Institutionen för slaviska och baltiska språk,
finska, nederländska och tyska

Riktlinjer för IT och IT-säkerhet

Filhantering

- Du som har Arbetsplatstjänst (SUA): Spara dina filer i din hemkatalog (Z:) på servern och inte lokalt på datorn. Då förlorar du inte dina filer även om din dator skulle gå sönder eller bli stulen. Genom att logga in på minafiler.su.se kan du komma åt filer i din hemkatalog.
- Du som inte har Arbetsplatstjänsten (SUA): Du ansvarar du själv för din säkerhetskopiering, exempelvis genom att förvara viktiga filer i en Box-synkad mapp (se nedan). Mac-användare kan använda backup-programmet TimeMachine mot en extern hårddisk, som självklart ska förvaras på annat ställe än datorn.
- Använd enbart molntjänsten Box som är upphandlad av Stockholms universitet om du har behov av molntjänster. Observera att känsliga personuppgifter aldrig ska behandlas i molntjänster, varken i Box eller i någon annan tjänst. Man ska vara försiktig med alla typer av personuppgifter i molntjänster. Var försiktig med hur du delar filer från Box: Det går att göra mappar och filer tillgängliga för hela världen, enbart för personer inom SU eller utvalda medarbetare. Dela bara filer via Box om du är helt säker på vad du gör!
- Kryptera filer med känslig information. Googla på ”kryptera filer” för tips. Det går att kryptera enskilda filer, t.ex. en PDF innan man skickar den via epost, eller en filarea där man i sin tur kan lagra filer, vilka därmed blir krypterade.

Åtkomst och inloggning

- Använd dig av starka lösenord. Det är särskilt viktigt att du har ett starkt och unikt lösenord till ditt universitetskonto, eftersom kontot ger tillgång till så mycket. Användarnamn och lösenord ska inte antecknas och lösenord måste bytas ut regelbundet. Se Stockholms universitets regler för lösenord i Serviceportalen. Du ska inte ha samma lösenord till flera resurser. Lösenordet till den egna datorn måste vara ett starkt lösenord.
- Låna inte ut ditt universitetskonto. Om du har gäster som behöver få tillgång till Stockholms universitets publika nät kan man beställa en engångskod (fråga Åke eller Laura).
- Lås alltid dörren när du lämnar ditt rum.

Stockholms universitet

- Lås alltid din dator när du lämnar ditt rum. Se till att din dator inte går att öppna utan lösenord efter viloläge; ställ in så att datorn kräver lösenord direkt eller högst efter 5 min.
- Lås dörren och stäng fönstren när du lämnar undervisningslokalen.
- Var restriktiv med personuppgifter: samla inte mer uppgifter än vad du verkligen behöver, var försiktig med listor med alla typer av personuppgifter, spara inte i onödan, använd Ladoks resultatnoteringar istället för papperslistor och filer när det går, dokument med personuppgifter ska inte kastas i pappersinsamlingen utan förstöras med dokumentförstörare. Även elektroniska lagringsmedier ska förstöras på rätt sätt om de har innehållit känsliga personuppgifter och inte längre ska användas.
- Använd inte öppna nätverk (ex. WIFI på kaféer eller hotell). Mobilnätet är tryggare, utnyttja därför möjligheten att koppla upp din dator via mobiltelefonen om du har mobilsurf. Se vidare om Eduroam.
- Det trådlösa nätverk som ska användas på arbetsplatsen är Eduroam, eftersom det är krypterat. Det öppna nätverket SU får inte användas. Installera Eduroam och du kan få nytta av det även på många andra ställen runtom i världen!
- Ladda inte ner okända filer och klicka inte på okända länkar. Om avsändaren är okänd och/eller om innehållet känns suspekt (ex. ber om inloggningsuppgifter, kräver snabb handläggning av ett ovanligt ärende, grammatiken är inkorrekt) ska man hantera meddelandet försiktigt. Häll muspekaren över länken utan att klicka (”hoovra”) för att se om länken leder till rätt plats. Svara inte på meddelandet utan skicka ett separat mejl till avsändaren om du misstänker att meddelandet inte kom från rätt person. Se Stockholms universitets information om bedrägeriförsök.
- Lär dig skilja mellan http och https i webbadresser: ”s” i https står för ”secure” och betyder att trafiken är krypterad. Lämna aldrig ut viktiga uppgifter på sajter som bara har http. Ett lösenord som används för inloggning till en http-sajt skickas i klartext, vilket är ytterligare en anledning att inte använda samma lösenord på flera sajter.
- Låt din dator göra de uppdateringar som operativsystemet kräver. Skjut inte upp och kontrollera emellanåt manuellt om det finns uppdateringar att göra.

Kommunikation

- Använda Mondo eller Athena eller forum för att kommunicera med studentgrupper. Gör du epostutskick till grupper ska du använda BCC-adressfältet (dold kopia) i e-postprogrammet; mottagarna ska inte få tillgång till varandras adresser.
- Din su.se-e-postadress ska användas i tjänsten och enbart i tjänsten. Tänk på att alla e-postmeddelanden är allmänna handlingar. Skaffa en privat e-postadress om du saknar en.
- Svara på e-post och andra förfrågningar så fort som möjligt. Myndighetens serviceskyldighet regleras i Förvaltningslagen. Använd dig av frånvaromeddelanden vid behov. Du kan även svara kort att du utreder ärendet och återkommer senare. Tänk även på att interna förfrågningar ska besvaras inom rimlig tid.

Stockholms universitet

- Kontrollera din skräppost en gång om dagen. Radera det som är skräp. E-post som är skräp men som inte markerats som skräp kan du själv märka, så att systemen lär sig till nästa gång.
- Välj inte ”svara alla” om du inte är säker på att alla behöver få ditt svar. Fundera också på vem verkligen behöver få ditt meddelande, skicka inte till många utan att tänka efter. Hjälp till att hålla ner mängden epost genom att bara skicka/vidarebefordra relevant info till relevanta mottagare. Var särskilt försiktig med e-postlistor, som har många medlemmar.
- När du skickar ärenden vidare: Redigera bort irrelevant info, så att mottagaren snabbt kan orientera sig. Ge korta läsanvisningar vid behov. Ta reda på skillnaden mellan ”Forward” (Vidarebefordra) och ”Redirect” (Eftersänd) och hur du kan använda det för olika syften.
- Om du jobbar med sociala medier i tjänsten: Bekanta dig med Stockholms universitets checklista för sociala medier och Stockholms universitets information om arbete i sociala medier.
- Om du fotar eller filmar i tjänsten: Alla personer som kan kännas igen på bilder och film måste tillfrågas och de behöver lämna ett skriftligt samtycke. Samtycket ska arkiveras på institutionen. Blanketten finns på Stockholms universitets webbsida. Bilderna och filmerna ska sparas på en gemensam server så att flera personer har tillgång till materialet. Fråga Laura om du undrar över något. Observera att andra regler gäller för forskningsmaterial.

Läs vidare

- Stockholms universitets sidor om säkerhet
- Stockholms universitets sidor om IT-säkerhet
- Stockholms universitets sidor om åtkomst
- Om GDPR: den nya dataskyddsförordningen, ”nya PUL”
- Serviceportalen: Mest IT-relaterad information men även annat. Bra ställe att söka instruktioner för vanliga installationer/inställningar. Du kan även göra beställningar och felanmälan här.

Sist men inte minst

- Fråga om något är oklart.
- Hjälp varandra, fråga varandra: kan du visa hur man krypterar en fil? Kolla, det där kan man göra på ett smartare sätt så här!
- Reagera om du ser tecken på osäker hantering.