Utgivare: Kommunledningsförvaltningen Kansli

Gäller från: Lagakraftvunnet beslut

Gäller till och med: tillsvidare

Antagen: Kommunstyrelsen 2019-03-26 § 95

Riktlinjer för IT och informationssäkerhet - användare

Inledning

IT- och informationssäkerhetspolicyn är det styrande dokument som anger Karlshamns kommuns förhållningssätt till och användande av informations- och kommunikationsteknik. Dokumentet klargör omfattning, roller och ansvar för IT-användning inom kommunens verksamheter.

Riktlinjer för IT och informationssäkerhet – användare ger kommunens medarbetare ramar inom vilka medarbetaren kan eller ska agera för att policyn ska upprätthållas.

Ditt ansvar som användare

Information är en grundläggande tillgång för att kunna bedriva vårt arbete i kommunen. Det är allas vårt ansvar att hantera informationen på ett korrekt sätt. Du som användare ansvarar för att informationen du använder och genererar är korrekt och laglig.

För stöd och hjälp när det gäller användningen av enskilda program kontaktar du aktuell systemförvaltare eller IT-support. Har du problem med din dator ska du kontakta IT-support.

Åtkomst till information

Behörighet
Våra informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt informationen som finns i dem. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs av din chef.

Inloggning
När du loggar in första gången får du ett tillfälligt lösenord av IT-support för åtkomst till det administrativa nätverket. Lösenordet ska du byta till ett personligt lösenord efter första inloggningen, då du blir uppmanad till detta av systemet. Samma förfarande gäller för enskilda informationssystem som kräver lösenord för åtkomst.

Lösenord är strängt personliga och ska hanteras därefter. Du får aldrig lämna ut dina inloggningsuppgifter eller försöka att logga in med någon annans identitet. Lösenord ska aldrig förvaras på din arbetsplats eller i dina arbetsverktyg.

Du lämnar spår efter dig när du är inloggad och arbetar i systemen. De loggningsfunktioner som finns i systemen används bl.a. för att spåra obehörig åtkomst. Detta för att skydda informationen och för att undvika att oskyldiga misstänks om oegentligheter inträffar. Loggarna kontrolleras regelbundet.

Om du glömmer ditt lösenord eller om ditt konto har spärrats (t.ex. genom för många felaktiga inloggningsförsök), ska du be din närmsta chef eller kollega kontakta IT-support för upplåsning av konto alternativt lösenordsbyte.

Använd inte dina inloggningsuppgifter (användaridentitet och lösenord) när du registrerar dig på externa webbplatser eller andra Internet-tjänster.

Val av lösenord

För AD-lösenord gäller att det ska:

- vara minst tio tecken långt
- bestå av en blandning av stora och små bokstäver, siffror.
- inte återanvändas
- inte baseras på repetitiva mönster så som ABC123 eller AAA111
- inte vara baserat på ett vardagligt ord (som förekommer i en ordlista) eller något som kan kopplas till dig som person t.ex. familjemedlems namn.

Tips: även om vardagliga ord ska undvikas går det att skapa lösenordsfraser som i sin helhet är lika bra i fråga om säkerhet som slumpmässiga teckenkombinationer men som är lättare att komma ihåg. Exempel på detta kan vara PappaKanAllt#98" eller K4llt0mV1ntern. Var dock noga med att inte använda just dessa två exempel!

Byte av lösenord
Byte av lösenord är aktuellt var 24:e månad eller på inrådan från IT & Teleservice.

För mobiltelefoner och surfplattor gäller att dessa alltid ska vara belagda med lösenkod. Detta regleras genom kommunens manageringsverkyg.

Din arbetsplats

Utrustning
För den utrustning som du förfogar över och som används för att hantera information i din tjänsteutövning (t.ex. stationär eller bärbar dator, mobiltelefon, USB-minnen, etc.) gäller följande:

Du är ansvarig för den utrustning som du förfogar över, vilket innefattar att:

- Hålla utrustningen under uppsikt eller inlåst.
- Hålla utrustning som inte används avstängd eller spärrad (t.ex. med lösenordsskydd).

För utrustning tillhandahållen av kommunen gäller följande:

- Utrustningen ska vara registrerad i kommunens inventariesystem och/eller managerad av kommunen. Klisterlapp med löpnummer för inventariet får inte tas bort.
- Fysiska ingrepp får endast utföras av IT-support eller annan auktoriserad person.
- Fel ska anmälas till IT-support.
- All installation/avinstallation och konfiguration får endast utföras av IT-support.
- Installation och konfiguration av hårdvara får endast göras av IT-support eller av annan anvisad/auktoriserad person.

Övrig utrustning betraktas som externa enheter och får inte anslutas direkt mot det administrativa nätverket. IT-support kan redogöra för vilka möjligheter det finns att komma åt information och verksamhetssystem via externa enheter.

Programvara

Allmänt gäller följande:

- Det är inte tillåtet att kopiera eller använda kommunens program utanför kommunens verksamhet.

För programvara som ska användas tillsammans med utrustning som ska anslutas direkt mot det administrativa nätverket gäller följande:

- Programvara ska godkännas och installeras av IT-support eller av IT-support anvisad/godkänd person.
- Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din chef som kontaktar IT-support.

Service på utrustning

Om du behöver lämna din utrustning för service ska all känslig information som är sparad lokalt på din dator (t.ex. på Skrivbordet) tas bort. Det är också viktigt att du ser till att inte ha dokument av värde sparade lokalt då dessa kan försvinna under servicen. Är du osäker kan du kontakta IT-support.

Avveckling av utrustning

IT-utrustning som inte används i verksamheten ska lämnas till IT & Teleservice.
Utrustning som ska avvecklas eller kasseras ska tas om hand enligt kommunens rutiner för detta, IT-support ombesörjer destruktion. IT-utrustning ska vid avveckling i första hand lämnas för återanvändning och i andra hand för bästa möjliga återvinning om inte reglerna för klassning av kommunens information säger annorlunda.

OBS - du får inte själv återvinna eller kassera din utrustning. Kontakta IT-support för hantering i dessa ärenden.

När du lämnar din arbetsplats

Vid tillfällen när du inte har uppsikt över din dator ska du tillfälligt låsa den.

Våra lokala nätverk

Våra datanätverk är mycket viktiga gemensamma resurser för alla medarbetare och ger oss möjlighet att bl.a. spara information, dela på skrivare, upprätta kommunikation och använda våra verksamhetssystem.

För att nätverken ska vara säkra gäller följande regler för arbete inom dem:

- Alla transaktioner på nätverken loggas och registreras.
- Utskrifter på en gemensam skrivare ska hämtas snarast. I de fall där det är möjligt ska ”säker utskrift” användas och skrivas ut på papper först när du aktivt gör det valet på skrivaren.
- Tillgång till kommunens nätverk från annan plats ska beställas genom itsupport@karlshamn.se. Ingen annan fjärråtkomstlösning får förekomma eller installeras.
- Du får inte utnyttja felkonfigureringar, programfel eller andra metoder för att skaffa dig utökade systemrättigheter eller annan personlig rättighet än den som har tilldelats dig av systemägaren.
- Du får inte arbeta destruktivt på nätverken (dvs. med avsikt att skada lagrad information).

Klassning och hantering av information

Klassning

Klassning av information ska göras i enlighet med bilaga 1.

Lagring

Den information du lagrar på våra gemensamma utrymmen säkerhetskopieras automatiskt. Du ska därför lagra din information i din egen hemkatalog (t.ex. F:), alternativt i verksamhetsgemensam katalog.

- Egen hemkatalog är ditt personliga arkiv som du ska använda för lagring av personlig information. De filer du sparar i din hemkatalog kan endast du nå.
- Gemensam katalog är ett arkiv för lagring av gemensam information för en förvaltning, avdelning eller ett arbetslag.

Allmänt gäller att du är ansvarig för att:

- inte lagra sekretessbelagd information på andra platser än anvisade IT-system för detta,

Observera att det du lagrar på din lokala hårddisk (C:, t.ex. på skrivbordet på din dator) inte automatiskt säkerhetskopieras, du är därför personligen ansvarig för säkerhetskopiering av den information du lagrar där. När du lagrar information på din lokala hårddisk riskerar du att förlora information som inte kan återskapas till rimliga kostnader, vid t.ex. en diskkrasch. Undvik därför att lagra på C:. Tänk också på att den information du lagrat på din lokala hårddisk är tillgänglig för alla som kan starta din dator. Man behöver ofta inte använda något lösenord för att komma åt dessa hårddiskar.

Långsiktig lagring ska inte göras på mobiltelefoner eller surfplattor. Information som ska bevaras ska överföras till diarium eller verksamhetssystem. Molntjänster som inte är godkända av kommunen får inte installeras eller användas på enheten.

Internet

När du använder Internet kan säkerheten i kommunens lokala nätverk påverkas i mycket hög grad beroende av ditt beteende. Kommunen förutsätter att den som surfar på Internet gör det med ansvar.

Det är inte tillåtet att upphovsrättsskyddat material laddas ner utan tillstånd eller att kränkande eller frånstötande material med inslag av t ex rasism, våld eller pornografi laddas ner, produceras, hanteras eller distribueras via e-post, internet eller telefoni. Undantag från detta kan beviljas av närmaste chef om materialet kan ha relevans för arbetsuppgifterna.

Tänk på att när du surfar på Internet representerar du Karlshamns kommun och lämnar spår efter dig, t ex i form av kommunens IP-adress.

E-post

För e-post gäller samma offentlighets-, sekretess- och arkivregler som för övriga handlingar. Den som tar emot och sänder e-post ska själv avgöra om e-posten är att betrakta som en allmän handling i lagens mening. **Allmänna handlingar ska registreras i kommunens diarium snarast.** Detta gäller både inkommande och utgående e-postmeddelanden inklusive eventuella bilagor. Kommunens dokumenthanteringsplan med beslutade gallringsfrister ska följas. Vid hantering av e-post ska även dataskyddslagstiftningen följas, vilket innebär att det ska finnas en rättslig grund för att behandla personuppgifter i e-post och att du som användare i övrigt har att förhålla dig till samma skyldigheter att informera, regler för säkerhet m.m. som vid annan personuppgiftsbehandling.

E-posten bör hanteras vardagligen och får inte lämnas orörd i inkorgen. Vid planerad frånvaro längre än en vardag ska din e-post vidarebefordras till för dig utsedd ersättare. Vid oplanerad frånvaro ska närmsta chef kontakta IT-support och tillse att e-posten vidarebefordras till en ersättare. Du kan också sätta ett frånvarobesked med uppgift om vem som kommer att hantera din inkommande e-post under din frånvaro. Observera att all e-post i din inkorg är att betrakta som inkommen till kommunen, oaktat om du läst den eller inte. Det är därför inte tillräckligt att under frånvaro skicka meddelande om att avsändaren ska vända sig någon annanstans, utan handlingen som kommit in måste antingen hanteras av dig eller en ersättare.

E-post är ett hjälpmedel i ditt arbete, men minneskapaciteten för den är begränsad. Tänk därför på att regelbundet rensa i din elektroniska brevlåda för att frigöra utrymme så att inte din e-post spärras.

E-postsystemet ska inte användas som ett arkivsystem. Meddelanden, bifogade filer m.m. som du vill spara, sparar du på samma sätt som du lagrar annan information.

Var selektiv med att skicka eller vidarebefordra meddelanden som innehåller stora filer för att undvika onödig belastning av systemresurser. Filer som är större än 20 Mb delas lämpligen på annat sätt än med e-post.

E-post med bilagor och länkar till webbplatser utgör ett stort hot när det gäller spridning av virus.

- E-postsystemet är ett arbetsverktyg och ska inte användas för privat bruk.
- Gör en bedömning av mottagna filer och bilagor innan de öppnas. Finns det anledning att misstänka att de kan innehålla något skadligt som t.ex. virus? Kontrollera med avsändaren ifall du är osäker på innehållet. Tror du att du mottagit en bilaga som inte bör öppnas ska du kontakta IT-support för hjälp vidare.
- Om du misstänker att det kommit in virus via e-postsystemet ska du agera som beskrivits i avsnittet om Incidenter.
- Det är inte tillåtet med automatisk vidarekoppling till extern e-postadress.
- Ange alltid ämne i ämnesraden för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-posten.
- Sekretessreglerade uppgifter och känsliga personuppgifter enligt dataskyddsförordningen får inte skickas via e-postsystemet, varken internt eller externt.
- Mottages sekretessreglerade uppgifter eller känsliga personuppgifter enligt dataskyddsförordningen via e-postsystemet ska informationen omgående flyttas till en lämplig plats, exempelvis diarium, personakt eller ärendehanteringssystem, samt raderas

från inkorgen och papperskorgen i e-postsystemet. Vid kontakt med enskilda eller andra myndigheter ska hänvisas till andra säkrare kontaktvägar.
- Skriv inte någon känslig information i ämnesraden.
- Tänk på att dölja mottagarna om du skickar e-post till flera externa mottagare som inte ska ta del av de andra e-postadresserna du skickar till.
- Vidarebefordra endast e-post till de personer som behöver ta del av informationen för att hantera ärendet.
- Kontrollera vilka som är medlemmar på sändlistor innan du använder dem. (Risk att känslig information når fel mottagare.)
- Använd endast ”läskvittens” för interna meddelanden när du har behov av detta.
- Tänk på hur du sprider din e-postadress.
- Får du hotbrev eller liknande ska du spara brevet och kontakta din chef.

Incidenter och virus m.m.

Allmänt
Om du misstänker att någon använt din användaridentitet eller att du varit utsatt för någon annan typ av incident ska du:
- notera när du senast var inne i IT-systemet
- notera när du upptäckte incidenten
- omedelbart anmäla förhållandet till närmsta chef och IT-support
- dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om kvaliteten på din information har påverkats.

Om du upptäcker fel och brister i de system du använder ska du rapportera dessa till IT-support samt din närmaste chef.

Virus
Utrustning tillhandahållen av kommunen har programvaror för viruskontroll både i klienterna och i nätverket, men kan ändå drabbas av effekter av s.k. skadlig kod. Om du misstänker att din dator innehåller virus ska du:
- Stänga av datorn och kontakta IT-support.

Om du får brev med virusvarning, kontakta IT-support.

Mobila enheter, digitala kameror m.m. kan lätt bli virusbärare eftersom du kan mellanlagra information mellan olika datorer i dessa. Var noga med att den dator du ansluter sådan kringutrustning till har ett uppdaterat virusprogram.

Avslutning av anställning

När du slutar din anställning i kommunen ansvarar du för att:
- rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas och var.
- privat material tas bort.
- återlämning av den utrustning du tagit del av för att fullgöra dina arbetsuppgifter.

Närmsta chef ansvarar för att de behörigheter för åtkomst till kommunens informationssystem en anställd har avbeställs när anställning avslutas.

Revidering och uppföljning

IT-chefen ansvarar för att årligen se över och vid behov ge förslag till kommunstyrelsen angående revidering av riktlinjerna för IT- och informationssäkerhet.

Bilaga 1: Informationsklassningsnivåer

Konfidentialitet - att informationen kan åtkomstbegränsas.

Riktighet – att information ska vara tillförlitlig, korrekt och fullständig.

Tillgänglighet – att information ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.

Spårbarhet – att specifika aktiviteter som rör informationen kan spåras.

Nivå 0 – Ingen eller försumbar skada

- Inga svårigheter för verksamheten att nå målen.
- Ingen eller endast försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation

Nivå 1 – Måttlig skada

- Inga märkbara större svårigheter för verksamheten att nå målen.
- Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.

Nivå 2 – Betydande skada

- Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).
- Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte.
- Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen.

Nivå 3 – Allvarlig skada

- Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.
- Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt.
- Individers liv och hälsa äventyras

Nivå 4 – Synnerligen allvarlig

- Röjande av informationen medför **skada för rikets säkerhet som inte endast är ringa.**
- Systemet behandlar information som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där röjande av information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger.
- Informationen omfattas av t ex säkerhetsskyddslagstiftningen