HAMMARÖ KOMMUN

2021-11-18

Kommunstyrelsen
IT-enheten

Utvecklingsledare IT

Informationsäkerhetsinstruktion Användare (Infosäk A)

Inledning

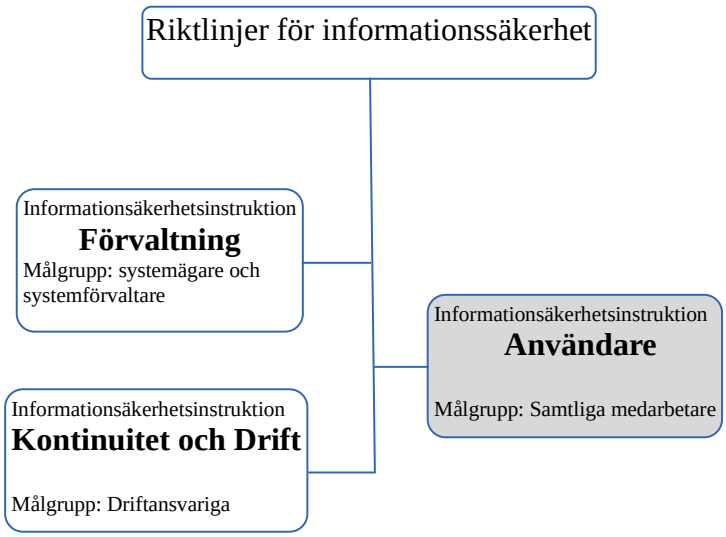
Med *informationssäkerhet* avses den samlade effekten av de skyddsåtgärder som tillsammans minskar eller eliminerar effekterna av hot och risker som riktar sig mot IT-stödet och informationstillgångarnas tillgänglighet, riktighet, sekretess och spårbarhet.

Med *information* avses här all information oberoende av i vilken form eller miljö den förekommer - den kan vara muntlig, skriven, tryckt eller elektronisk. Då datorer och IT-system idag har en så central roll som bärare av information blir denna instruktion dominerad av frågor rörande detta.

Styrande dokument för arbetet med informationssäkerhet i Hammarö kommun är Riktlinjer för informationssäkerhet med tillhörande instruktioner.

Denna Informationssäkerhetsinstruktion för användare (**Infosäk A**) redovisar hur en användare ska verka för att upprätthålla en god säkerhet.

Instruktionens roll i informationssäkerhetsarbetet



Riktlinjer för informationssäkerhet redovisar fullmäktiges viljeinriktning och mål för informationssäkerhetsarbetet. Riktlinjen konkretiseras i informationssäkerhetsinstruktioner.

Informationssäkerhetsinstruktion Förvaltning (Infosäk F) redovisar:

- den interna organisationen för informationssäkerhetsarbetet
- de olika rollernas ansvar
- hur informationssäkerhetsarbetet skall bedrivas

Informationssäkerhetsinstruktion Kontinuitet och drift (Infosäk KD) redovisar:

- organisation och ansvar för drift av informationssystem
- regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering

Användarens ansvar

Information är en viktig tillgång för Hammarö kommun. För att skydda denna krävs ett säkerhetsmedvetande hos alla medarbetare. Som användare har du alltså en del i ansvaret för säkerheten i informationshanteringen.

Vid hantering av personuppgifter ska hänsyn tas till PUL, personuppgiftslagen (efter 20180525 GDPR/DSF). Information om detta finns på intranätet (Insidan):

Dataskyddsförordningen

För stöd och hjälp när det gäller användningen av enskilda program kontaktar du aktuell systemförvaltare. De olika ansvariga framgår av förteckningen på intranätet:

Verksamhetssystem och ansvar

Har du problem med din datorutrustning ska du kontakta IT-support på intranätet:

Supportsidan - Hammarö kommun

Åtkomst till information

Behörighet

Våra informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kan använda dessa. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs av din chef.

Inloggning

Chef, eller av denne utsedd person, registrerar anställningsuppgifter i kommunens personalsystem. När din anställning i kommunen träder i kraft erhåller du behörighet till kommunens nätverk, hemmakatalog, intranätet, Internet, utskrifter, generella IT-system samt e-post. Din chef får dina inloggningsuppgifter i ett mejl. Första gången som du loggar in med det tilldelade lösenordet i nätverket byter du omedelbart lösenord till ett lösenord som bara du känner till. Det är vanligt att den principen används som första åtgärd för nya IT-system som du får behörighet till, nämligen att du får ett preliminärt lösenord som du vid första inloggningen omedelbart ska byta. Om du har glömt lösenordet till Nätverket så behöver du kontakt din chef som kan bistå med ett nytt tillfälligt lösenord.
Systemansvarig för respektive system ansvarar för att ge dig behörighet till de verksamhetsspecifika system som du använder i arbetet. Användarnamn och lösenord distribueras till dig antingen via din chef eller från din systemansvarig per epost.

Val av lösenord

Lösenordet som är kopplat till ditt användarnamn, är till för att förhindra obehöriga från att få tillgång till kommunens information. Vissa system/applikationer har regler för hur lösenordet ska vara konstruerat, andra tillåter ”enklare” lösenord. Tänk dock på att om du väljer ett enkelt lösenord underlättar du för eventuella angripare att ta sig in i kommunens nätverk och system.

Tänk på detta då du väljer lösenord:

- Lösenord är personliga och det är ditt ansvar att se till att ingen annan känner till dina lösenord.

- Du bör lära dig lösenordet utantill, om du behöver dokumentera lösenordet så skall detta ske på ett säkert sätt.

- Lösenordet ska vara minst 8 tecken långt och uppfylla minst 3 av följande kriterier:

  Innehålla minst en versal (stor bokstav)
  Innehålla minst en gemen (liten bokstav)
  Innehålla minst en siffra 0–9
  Innehålla minst ett specialtecken (!*#...)

- Använd inte heller namn på familjemedlemmar, husdjur, telefonnummer el dylikt som kan kopplas till dig personligen.

- Du får inte använda samma lösenord i kommunens system som de du använder hemma.

Byte av lösenord

Du kan själv när som helst byta lösenordet till datorn genom att trycka Ctrl-Alt-Del och välja Ändra lösenord.

För enskilda IT-verksamhetssystem byts lösenordet efter ett visst tidsintervall som bestäms av respektive systemförvaltare.

Vid misstanke om spridning av lösenord skall det omedelbart bytas!

Din arbetsplats

Utrustning

Privat användning av kommunens utrustning får endast ske i undantagsfall, med sunt förnuft och på ett sätt som inte innebär extrakostnader för kommunen. Det kan röra sig om något enstaka privat samtal av kortare karaktär, enstaka SMS eller kortare användning av internet. Vad som menas med ”enstaka” och ”kortare” avgörs vid behov av arbetsgivaren utifrån en skälighetsbedömning.

Programvaror
Utöver de standardprogramvaror som alla har tillgång till, som till exempel e-post, tilldelar din chef dig de programikoner som du behöver i ditt arbete.

Service på utrustning
Vid behov felanmäler du enligt ovan till IT-supporten.

Kassering av utrustning
Utrustning som ska kasseras ska återlämnas till IT som säkerställer att känslig information inte sprids innan återvinning.

Om du lämnar arbetsplatsen
Vid tillfällen när du inte har uppsikt över arbetsstationen ska du tillfälligt låsa datorn med kortkommando: CTRL+ALT+DEL och ENTER

Klassning och hantering av information

Klassning av information

Information i Hammarö kommuns förvaltningar och bolags verksamhetssystem och annan lagring klassas utifrån den information som hanteras. Klassning görs från aspekterna konfidentialitet (sekretess), riktighet, tillgänglighet och spårbarhet.

Med detta menas:

Konfidentialitet: Att informationen skyddas från obehörig insyn
Riktighet: Att informationen inte ändras på ett obehörigt sätt
Tillgänglighet: Att informationen finns tillgänglig för rätt person vid rätt tillfälle
Spårberhet: Att förändringar i informationen kan synliggöras avseende vem, vad och när.

Flyttas information och lagras på andra media, eller används i ett annat sammanhang, måste den klassas där den används och hanteras därefter.

Även information i arbetsmaterial måste klassas.

Hammarö kommuns klassningsmodell framgår av bifogad bilaga.

Lagring

Se bilaga.

Instruktionens förhållande till Jämställdhetsplan

Kommunens arbetsplatser och utrustning ska vara fria från bilder, symboler, tidningar, skärmsläckare, informationsmaterial, utrustning m.m. som kan uppfattas som hotfulla, pornografiska eller på annat sätt könskränkande eller har med etnisk tillhörighet, religion, annan trosuppfattning eller brottslighet att göra.

Olämplig användning av utrustning och nätverk

När du använder Internet kan säkerheten i kommunens lokala nätverk påverkas i mycket hög grad beroende på ditt beteende. Kommunen som arbetsgivare förutsätter att den som surfar på Internet endast besöker välrenommerade webbplatser.

Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, etc.) eller har anknytning till kriminell verksamhet. Det är heller inte tillåtet att använda arbetstid till sådant.

I specifika fall kan det dock vara motiverat för arbetet, t ex vid utredningar, omvärldsanalyser mm, att besöka sidor som normalt är förbjudna. Beslut om detta ska fattas av närmaste chef.

Tänk på att när du surfar på Internet representerar du Hammarö kommun och lämnar spår efter dig i form av Hammarö kommuns IP-adress.

I de fall sådana sidor besöks för arbetets räkning ska chefen först informeras för att undvika missförstånd.

Vad som menas med pornografiska, rasistiska och diskriminerande webbsidor avgörs vid behov av arbetsgivaren.

Vid välgrundade misstankar om missbruk kan utredning på enskild utrustning ske i samråd med berörd förvaltningschef. En förutsättning är att användaren meddelas i förväg, innan utredning sker.

Missbruk kan leda till krav på ekonomisk ersättning från arbetsgivarens sida och/eller rättsliga åtgärder.

Vid misstanke om brott ska anmälan ske till polisen.

E-post

E-post är ett rationellt hjälpmedel i arbetet men minneskapaciteten för det är begränsad. Tänk därför på att regelbundet radera i mapparna "Inkorgen", "Skickat", och "Borttaget" för att frigöra utrymme så att inte din e-post spärras. Epostsystemet ska inte användas som ett arkivsystem. Meddelanden, bifogade filer mm 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.

Om du under en längre period inte har möjlighet att kontrollera din e-post ska du sätta frånvarobesked med eventuell uppgift om vem som ska hantera dina inkommande ärenden. Instruktion för detta finns i guiderna på supportsidan.

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

- epostsystemet är ett arbetsverktyg och bör inte användas för privat bruk.
- samma regler gäller för diarieföring av e-post som för vanliga brev.
- om du misstänker att det kommit in virus via epostsystemet ska du agera som beskrivits i avsnittet om Incidenter.
- ange alltid ämne i ämnesraden för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-posten.
- skriv inte någon känslig information i ämnesraden
- kontrollera vilka som är medlemmar på sändlistor innan du använder dem. (Risk att känslig information når fel mottagare)
- skriv korta brev
- använd "läskvittens" för interna meddelanden endast när du har behov av detta
- skicka inte eller vidarebefordra kedjebrev
- tänk på hur du sprider din e-postadress
- om du får hotelsebrev ska du spara brevet och kontakta din chef.

Observera: Epostsystemet får inte användas för att skicka sekretessbelagd information.

Incidenter, virus mm

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 IT-chefen och din chef.
- 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, din närmaste chef eller Utvecklingsledare IT.

Virus

Hammarö kommun 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:

- dra ut nätverkskabeln, men låta datorn vara på
- omedelbart anmäla förhållandet till endera IT-chefen, IT-säkerhetssamordnaren, IT-suppport eller till närmaste chef. OBS! Anmälan ska ske per telefon eller besök, inte per e-post.

Om du får epost med virusvarning gör inget annat än kontakta IT-support.

Handdatorer, digitala kameror, mobiltelefoner mm 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 ansvarar du för att:

- rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas. Notera att allt arbetsmaterial du framställt anses vara Hammarö kommuns egendom och får inte tas med utan chefs godkännande.
- privat material tas bort.
- de behörigheter du fått för åtkomst till våra informationssystem avbeställs av din chef.
- id-handlingar och nycklar återlämnas.

Denna Informationssäkerhetsinstruktion för användare inklusive bilagor är:
Fastställd av

_____

Caroline Depui, kommundirektör
2021-11-18

Bilaga – Klassning av information

Information som hanteras i verksamhetssystem eller annan lagring.

För information som lagras i IT-system, gruppkatalog eller personlig mapp måste inte bara sekretessaspekten beaktas, utan även kraven på riktigheten i informationen, tillgängligheten till den och spårbarheten.

Säkerhetsaspekt / Kravnivå	**Sekretess (konfidentialitet)**	**Riktighet**	**Tillgänglighet**
Mycket hög nivå **Nivå 3**	Information som kan medföra **mycket allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **mycket allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som ska vara åtkomlig **inom högst 2 timmar** för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person
Hög nivå **Nivå 2**	Information som kan medföra **allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som inte behöver vara åtkomlig inom 2 timmar, men **inom högst 8 timmar** för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person
Basnivå **Nivå 1**	Information som kan medföra **mindre allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **mindre allvarliga** negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som inte behöver vara åtkomlig inom 8 timmar för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för

Anm: Följande typ av information hanteras utanför klassningsmodellen:

- Information som avser rikets säkerhet. Sådan information ska hanteras enligt särskilda bestämmelser.

- Information som har extrema krav på sig att vara tillgänglig och där utgångspunkten är att den alltid ska vara det.
- Information som inte bedömts ha krav på sig vare sig avseende konfidentialitet, riktighet eller tillgänglighet.

Information på datamedia

Med datamedia menas CD/DVD, USB-minnen, externa hårddiskar, mobiltelefoner, digitalkameror och annan utrustning som det går att kopiera information till. Dessa medier ska inte ses som slutliga förvaringsformer, såvida de inte avser backup-tagning. Information på datamedia är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån. Eftersom informationen är kopierad behöver endast kraven på sekretess (konfidentialitet) beaktas. De krav på sekretess som ställs för ett specifikt IT-system framgår av användarhandledningen för systemet.

För information på datamedia gäller följande krav:

Krav på sekretess	**Åtgärder**
Mycket hög nivå	Förvaring – Endast CD/DVD, USB-minnen eller extern hårddisk får användas och ska förvaras inlåsta Kopiering – Får kopieras endast med godkännande från systemägaren för systemet som informationen kommer ifrån Återanvändning – Får inte återanvändas Destruktion – Lämnas till IT för destruktion
Hög nivå	Förvaring – Endast CD/DVD, USB-minnen eller extern hårddisk får användas och ej förvaras synligt Kopiering – Får kopieras i samråd med systemets förvaltare/administratör Återanvändning – Tillåten Destruktion – Lämnas till IT för destruktion
Basnivå	Förvaring – Inga krav Kopiering – Tillåten Återanvändning – Tillåten Destruktion – Krävs ej

Information på andra media

Med andra media menas papper, film, OH-bilder etc. Information på dessa media är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån. Eftersom informationen är kopierad behöver endast kraven på sekretess (konfidentialitet) beaktas. De krav på sekretess som ställs för ett specifikt IT-system framgår av användarhandledningen för systemet.

För information på ovanstående media gäller följande krav:

Krav på sekretess	Åtgärder
Mycket hög nivå	Förvaring – Förvaras inlåsta Kopiering – Får kopieras endast med godkännande från systemägaren för systemet som informationen kommer ifrån Återanvändning – Får inte återanvändas Destruktion – Papper och OH-film destrueras i papperstugg – Övrigt lämnas till IT för destruktion
Hög nivå	Förvaring – Ej förvaras synligt Kopiering – Får kopieras i samråd med systemets förvaltare/administratör Återanvändning – Tillåten Destruktion – Lämnas till IT för destruktion
Basnivå	Förvaring – Inga krav Kopiering – Tillåten Återanvändning – Tillåten Destruktion – Krävs ej