Program Plan Policy Riktlinje

Riktlinje informationssäkerhet - medarbetare

Beslutad av: Kommunstyrelsen
Datum och paragraf: 2023-10-03, § 192
Dokumentansvarig: Administrativ chef
Revisionsdatum:
Dnr: 23KS48

Innehåll

1 Inledning

Information är en viktig tillgång och en förutsättning för att kommunen ska kunna bedriva verksamhet. Kommunens informationstillgångar måste därför hanteras på ett tillfredsställande sätt utifrån tre informationssäkerhetsaspekter:

- att information enbart är tillgänglig för behöriga (konfidentialitet)
- att information är korrekt, aktuell och fullständig (riktighet)
- att information är åtkomlig i rätt tid och användbar (tillgänglighet)

Dessa regler gäller i tillämpliga delar såväl muntlig som skriftlig information, oavsett media (papper, film mm).

2 Grundläggande riktlinjer

Uppträd som en god representant för kommunen. Den elektroniska utrustningen, datornät och e-post är arbetsredskap som används i tjänsten.

- För att vinna och behålla medborgarnas förtroende är det nödvändigt att arbeta med god etik och gott omdöme.
- Aktuella lagar och föreskrifter ska följas. Dessutom får det man gör inte väcka anstöt eller på annat sätt såra eller skada någon annan.
- Det är förbjudet att i kommunens utrustning hantera pornografi, rasistisk propaganda, hot, förtal, uppmaning till droganvändning, våld eller diskriminering eller liknande som strider mot lag, avtal samt demokratiska grundprinciper.

Tänk på säkerheten. Det är viktigt att säkerställa att information inte förvanskas, förstörs eller kommer i orätta händer.

- Håll inloggningsuppgifter hemliga och lämna aldrig ut dem till någon annan.
- Lås alltid enheter med skärm- eller tangentbordslås när du lämnar dem utan uppsikt.
- Lagra alltid informationen på kommunens servrar, inte på lokal hårddisk och inte på moln-/internetbaserade lagringstjänster om de inte är godkända av kommunen.

Arbetsgivaren kan göra kontroller. För att kontrollera att gällande regler följs har arbetsgivaren rätt att utan att underrätta användaren i förväg logga/kontrollera/granska enskilda användares elektroniska utrustning.

Om förvaltningarna har ytterligare säkerhetsregler så informerar ansvarig chef om detta.

3 Användaridentitet och lösenord

Användaridentiteten och lösenordet identifierar dig när du använder den elektroniska utrustningen. Du är ansvarig för allt som händer ”i ditt namn”.

- Ett lösenord ska så långt som möjligt vara ”starkt” och helst innehålla minst 8 tecken. Blanda små och stora bokstäver, siffror och specialtecken.
- Använd gärna 2-faktorsinloggning där det är möjligt.
- Lösenord är strängt personliga. Lämna därför aldrig ut ditt lösenord! Skriv inte upp lösenordet eller låt någon se dig över ryggen när du loggar in. Dela inte lösenord med andra.
- Använd olika lösenord för olika tjänster. Använd inte samma lösenord i jobbet som du har privat. Återanvänd inte hela eller delar av tidigare lösenord. Byt lösenord ofta.
- Låt inte webbsidor spara lösenordet. Får du frågan om lösenordet ska sparas, svara alltid Nej.
- Undvik ”säkerhetsfrågor”. De kan fungera som bakdörr till kontot.
- Om fel lösenord använts för många gånger så låses datorn. Kontakta Sydnärke-IT.

4 Behörigheter

Medarbetarens anställning utgör grunden för de behörigheter som tilldelas i syfte komma åt nödvändig information för att kunna utföra sina arbetsuppgifter. Vid behov är det den anställdes chef som ansöker om ytterligare behörigheter till berörd informationsägare/objektsägare.

5 Mobila enheter

Den IT-utrustning som tillhandahålls av kommunen kan vara stationär eller mobil. Exempel på mobila enheter är smarta telefoner, surfplattor, USB-minnen och externa hårddiskar. Kommunens mobila enheter ska vara anslutna till kommunens Mobile Device Management system (MDM).

5.1 Hantering av mobila enheter

- Mobila enheter som tillhandahålls av kommunen som personliga arbetsredskap får inte lånas eller överlåtas om det inte är enheter som delas av flera.
- Uppsatta säkerhetsinställningar i enheter får inte ändras eller tas bort.
- Installerad programvara får inte kopieras eller installeras på annan enhet.
- Mobila enheter ska låsas med lösenord.
- Känslig eller sekretessbelagd information får inte lagras på mobila enheter.
- Endast godkända programvaror får installeras på enheten.
- Endast av kommunen godkänd utrustning får anslutas till kommunens interna nät.
- Privat utrustning hänvisas till kommunens wifi gästnät.
- Undvik anslutning till externa trådlösa nätverk som till exempel hotell wifi.

5.2 Distansarbete

- Kommunens mobila enheter är utrustade för distansarbete. Arbete utanför kontoret ställer krav på säkert och medvetet beteende.

5.3 Fysisk hantering av mobila enheter

- Försiktighet ska iakttas vid arbete i publika miljöer. Arbete med känslig eller sekretessbelagd information får inte ske i publika miljöer.
- Mobila enheter får inte lämnas utan uppsikt i publika miljöer.
- Förlust av enhet ska omedelbart anmälas till Sydnärke-IT och närmaste chef. I vissa fall finns möjligheter att fjärradera information.
- Vid avslut av anställning ska mobila enheter överlämnas till närmsta chef.
- Utrustningen ska vårdas och hanteras på ett aktsamt sätt.

5.4 Särskilda regler för mobila enheter

Förutom de regler som gäller allmänt för mobila enheter gäller även följande vid användning av mobila enheter:

- Information som är känslig eller sekretessbelagd får inte hanteras i mobila enheter om inte särskild av kommunen godkänd säkerhetslösning används.
- Pinkoder, fingeravtryck eller annan autentisering måste användas till mobila enheter.
- Vårda utrustningen och använd exempelvis skärmskydd och skal.

6 Skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller ett nätverk utan administratörens samtycke och har utvecklats i syfte att störa IT-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i IT-utrustning.

- Skadlig kod kan spridas till dator eller mobila enheter om man öppnar bilagor i e-post, importerar filer eller surfar på Internet och klickar på fel länkar, inklusive sådana som finns i sociala medier.
- Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
- Var misstänksam och undvik att klicka på konstiga länkar eller fyll i irrelevanta uppgifter.
- Öppna bifogade filer endast om de kommer från känd avsändare och bilagan är förväntad. Tänk på att virusspridning kan ske via någons adressbok så även om avsändaren är känd kan det innehålla skadlig kod.
- Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod, stäng av enheten och kontakta Sydnärke-IT servicesdesk.

7 Sociala medier

Information som är känslig eller sekretessbelagd får inte hanteras i sociala medier. Inte heller känsliga personuppgifter. Kommunens användning av sociala medier kommer att regleras i Riktlinjer för sociala medier.

8 E-post

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom kommunen och till externa parter. Det är dock viktigt att tänka på att meddelanden i e-posten är oftast att betraktas som allmän handling. Kommunens e-post får inte användas för privata ändamål.

Kommunens användning av e-post regleras av Rutiner för posthantering inom Askersunds kommun.

9 Lagring och säkerhetskopiering

Det är viktigt att information sparas på ett säkert sätt eller arkiveras och säkerhetskopieras så att den kan återskapas. Lagring av information kommer att regleras i Riktlinjer för lagring av information.

10 Spårbarhet och loggning

Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när och följa förloppet för olika händelser på datorn.

11 Säkert beteende

En stor del av kommunens information hanteras muntligt och på papper. En del av denna information är särskilt skyddsvärd, känslig eller sekretessbelagd.

11.1 Muntlig information

- Känslig eller sekretessbelagd information har en begränsad krets av behöriga. Man ska enbart tala om detta i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.

11.2 Information på skärmar och i pappersform

- Internt skriftligt material på papper eller dataskärm kan vara känslig information och bör inte hanteras eller lämnas så att obehöriga kan läsa den. Låt till exempel ingen läsa över din axel, ta del av information genom ett fönster eller bilrutan och placera datorskärmar så att ingen obehörig kan ta del av informationen på skärmen.
- Material som innehåller känslig eller sekretessbelagd information ska låsas in i godkända skåp när man lämnar arbetsplatsen, även för kortare stunder.

- Känslig eller sekretessbelagd information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund. Om man har ett tjänstekort till datorn ska detta tas ut då man lämnar arbetsplatsen.
- Vid utskrift av dokument skall detta ske med hjälp av tjänster för säker utskrift där dokumenten skrivs ut först när mottagaren begär det.
- Besökare får inte vistas utan uppsikt i lokaler där känslig eller sekretessbelagd information kan finnas.
- Vid fysisk posttjänst bör rekommenderade försändelser användas om brev innehåller känslig eller sekretessbelagd information.
- Då känslig eller sekretessbelagd information överförs via fax ska man försäkra sig om att man har rätt nummer och att mottagarens fax är övervakad under överföringstillfället.
- Pappersdokument som innehåller känslig eller sekretessbelagd information måste vid kassering strimlas eller kastas i godkända säkerhetskärl.

12 Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänkts kunna medföra negativ påverkan på kommunens information till exempel:

- IT-angrepp/intrång
- Skadlig kod
- Oskyddad känslig information
- Brister i efterlevnad av lagar och regler för informationssäkerhet

Säkerhetsincidenter och personuppgiftsincidenter ska anmälas via riktlinjer och rutiner som följer gällande lagar och regler.