2025-04-08

Dnr: KSON 2025-227

Förvaltningens informationssäkerhetsinstruktion

Beslut

Beslutar att Kommunalförbundet Sjukvård och omsorg i Norrtäljes (KSON:s) förvaltning antar Norrtälje kommuns informationssäkerhetsinstruktion som sin egen.

Ann-Sophie Holgersson
Förbundsdirektör

Sammanfattning

Då Kommunalförbundet Sjukvård och omsorg i Norrtäljes (KSON:s) förvaltning huvudsakligen verkar i Norrtälje kommuns informationssystem behöver förvaltningens medarbetare följa kommunens informationssäkerhetsinstruktion.

Bilaga

Informationssäkerhetsinstruktion, Norrtälje kommun (KS 2021-193).

NORRTÄLJE KOMMUN

2021-02-01
Diarienummer: KS 2021-193

AVDELNINGEN FÖR SÄKERHET OCH KRISBEREDSKAP

Namn: Olof Sigfrid
E-post: olof.sigfrid@norrtalje.se

Informationssäkerhetsinstruktion

Information är en av Norrtälje kommuns viktigaste tillgångar och hur den hanteras är en mycket viktig del i arbetet. Reglerna i detta dokument är riktade till alla som på ett eller annat sätt bereds tillgång till och behandlar information tillhörande Norrtälje kommun, oaktat om informationen är i fysisk eller digital form. Det gäller så väl medarbetare, förtroendevalda, konsulter, leverantörer som kunder.

I denna instruktion beskrivs hur du som medarbetare ska arbeta med kommunens informationstillgångar, för att efterleva de rutiner och riktlinjer som finns fastställda, för att kommunen ska uppnå de mål som är fastställda för informationssäkerhetsarbetet.

1. Syfte och mål

Kommunens syfte med informationssäkerhetsinstruktioner är att skydda kommunens information.

2. Säkerhetsansvaret

Det är alltid varje enskild användares, både interna och externa, eget ansvar att tillgodogöra sig den fastställda informationssäkerhetspolicyn, riktlinjer, rutiner och instruktioner för hur man ska arbeta för att stödja kommunens informationssäkerhetsarbete.

Om du som enskild användare är osäker på hur information ska behandlas avseende säkerhet ska du vända sig till antingen informations- eller systemägare. Vem som är informations- eller systemägare finns beskrivet på kommunens intranät.

3. Åtkomstkontroll

Kommunens informationssystem har åtkomstkontroller för att säkerställa att endast behöriga användare får åtkomst till informationen.

3.1. Behörigheter

De behörigheter du har rätt till beror på din roll och dina arbetsuppgifter och tilldelas av din chef. För politiker tilldelas behörigheter av nämndsekreterare. Det finns en process för ansökan om behörighet som ska följas.

Kommunen arbetar utefter principen "need to know-basis", vilket innebär att en användare ska ha tillgång till endast den information som arbetsuppgifterna kräver.

	Hanteringsregler av behörigheter
3.1.1	Behörigheter till medarbetare ska beställas av närmaste chef.
3.1.2	Behörighetsbeställningar ska ske enligt IT- avdelningens process för behörigheter.
3.1.3	Chefer och nämndesekreterare är ansvariga att säkerställa att medarbetare och politiker har korrekt behörigheter.
3.1.3	Om du som medarbetare märker att du har åtkomst till information du är obehörig till ska detta informeras till närmaste chef. Chefen ska därefter anmäla detta vidare till IT och systemägare enligt process för behörigheter.

3.2.2.4	E-tjänstekortet ska alltid bäras synligt i kommunens kontorslokaler.
3.2.2.4	Om du förlorar ditt e-tjänstekort ska du kontakta Kontaktcenter och Telia omedelbart för att spärra kortet.

3.2.2. Lösenord

Som användare av IT-resurser vid Norrtälje kommun ansvarar du själv för att dina lösenord håller den kvalitet som anges i kommunens lösenordspolicy, att du håller dina lösenord hemliga, och som konsekvens av detta aldrig uppger dina lösenord för någon. Ingen har rätt att begära dina lösenord, och du har inte rätt att uppge dem.

En avgörande skillnad på ifall ett lösen ord är säkert beror på antalet tecken i lösenordet. Detta är anledningen till varför Norrtälje kommun valt att lösenordet ska vara minst 15 tecken långt.

Ett lösenord med 15 tecken kan förefalla svårt att skapa och memorera men det finns metoder som förenklar skapandet av bra lösenord och som är lätta att memorera. En metod är att att välja ut en mening och byta ut enstaka bokstäver till siffror och specialtecken. Ett sådant lösenord är nästan lika lätt att minnas som ett lösenord med endast fyra tecken.

Exempel lösenord:
Valet av meningen "Alltid kul på jobbet!" kan med byte av tecken bli till lösenordet:

alltiD 5 kul på jobbet!

Ett lösenord innehållande 23 tecken inklusive blanksteg (ja, blanksteg kan användas i lösenord)

Obs. lösenordet i exemplet får ej användas – skapa egna!

	Hanteringsregler för lösenord
3.2.2.1	Första gången du beviljas åtkomst till ett eller flera av kommunens informationssystem blir du tilldelad ett lösenord. Lösenordet ska alltid bytas till ett personligt lösenord efter första inloggningen.
3.2.2.1	Lösenord är personliga och får aldrig delas med någon annan.
3.2.2.3	Lösenordet ska vara unikt och inte användas i något annat system, vare sig inom kommunen eller utanför.

	Hanteringsregler av IT-utrustning
4.1.1	Endast av kommunen tillhandahållen eller godkänd IT-utrustning får användas för arbete i tjänsten.
4.1.2	För den IT-utrusning som du erhållit gäller följande; • fel ska omgående anmälas till IT-supporten, och • vid stöld eller förlust av IT-utrusning måste detta omedelbart rapporteras till IT-supporten och dataskyddsombudet.
4.1.3	Vid flytt av dator eller annan utrustning ska detta genast anmälas till IT-supporten.
4.1.4	När du tillfälligt lämnar din arbetsplats ska du låsa din dator för att förhindra obehörig åtkomst. Datorn ska även ha automatisk låsning efter 5 minuters inaktivitet.
4.1.5	När du lämnar din arbetsplats för dagen så ska du stänga av din dator.
4.1.6	IT-utrustning ska förvaras inlåst. Detta gäller i synnerhet bärbara datorer, läsplattor och mobiltelefoner.
4.1.7	När en användare inte behöver sin IT-utrustning längre ska användaren se till att ingen information finns kvar lagrad på enheten.

5. Informationsklassificering

Samtliga informationstillgångar som hanteras inom Norrtälje kommuns verksamhet ska klassificeras utifrån behov av konfidentialitet, riktighet och tillgänglighet för informationen enligt de klasser som beskrivs nedan. Med informationstillgång menas information som är skyddsvärd.

Klassificeringen är viktig för att informationen ska få ett tillräckligt skydd.

5.1. Konfidentialitet

Med konfidentialitet avses informationens behov av skydd mot obehörig åtkomst. Varje medarbetare, leverantör och övriga som hanterar kommunens skyddsvärda informationstillgångar måste beakta behovet av konfidentialitet i det dagliga arbetet, exempelvis då man avgör huruvida en viss informationsmängd får skickas med e-post.

ÖPPEN	INTERN	KÄNSLIG	HEMLIG
Med öppen information avses uppgifter som inte omfattas av några krav på konfidentialitet och därför inte behöver skyddas från att någon obehörig tar del av den.	Med intern information avses uppgifter som behöver ges ett grundläggande skydd mot obehörig åtkomst.	Med känslig information avses uppgifter som behöver ges ett särskilt skydd då obehörig åtkomst till uppgifterna skulle kunna innebära allvarliga konsekvenser för kommunen eller enskilda.	Med hemlig information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, där obehörigt röjande av uppgifterna kan medföra skada för Sveriges säkerhet.

För en sammanställning och en mer detaljerad beskrivning av informationsklassificeringsnivåer och med exempel på informationstyper för att underlätta för användare i klassificeringsarbetet, se dokumentet *Anvisning för informationsklassificering*.

5.2. Riktighet

Informationens riktighet är avgörande för såväl Norrtälje kommuns verksamhet som allmänheten och medias förtroende för kommunen. Riktigheten säkerställs främst genom en strikt tillämpning av behörighet att påverka informationsmängder i Norrtälje kommuns IT-miljö och åtgärder för att säkerställa spårbarhet (och därmed möjlighet att utkräva ansvar) då åtgärder vidtas i IT-miljön. Läs mer i *Riktlinje för systematiskt säkerhetsarbete.*

5.3. Tillgänglighet

Krav på informationens tillgänglighet utgår ifrån vilka konsekvenser det kan innebära för verksamheten om en viss informationsmängd är otillgänglig för behöriga användare. Konsekvensernas omfattning och hur tidskritisk informationen är för verksamheten är avgörande för vilka åtgärder som måste vidtas för att säkerställa tillgängligheten. Läs mer i *Riktlinje för systematiskt säkerhetsarbete.*

säkerhet. Vidare är det respektive systemägare som beslutar om distansarbete får ske för ett visst informationssystem.

	Regler för distansarbete
7.1	Vid distansarbete ska du se till att skydd finns mot insyn från obehöriga.
7.2	Du ska visa särskild aktsamhet vid hantering av bärbar utrustning och inte lämna dessa utan uppsikt.
7.3	Känsliga uppgifter ska inte behandlas via öppnat nät eller wifi på offentliga platser.
7.4	Vid utskrift av känsliga uppgifter utanför kommunens lokaler är det särskilt viktigt att obehöriga inte kan tillskansa sig uppgifterna.
7.5	Åtkomst till kommunens information får endast ske genom av IT-enheten tillhandahållen lösning.
7.6	Du ska säkerställa att den senaste versionen av skydd mot skadlig programvara finns installerad och att applikationer på IT-utrustning är uppdaterad.

8. Internet och E-post

8.1. Internet

När du använder Internet så är ditt agerande avgörande för säkerheten i kommunens lokala nätverk. När du surfar på Internet via kommunens nät representerar du kommunen och lämnar spår efter dig i form av en IP-adress som tillhör kommunen.

	Regler för användandet av kommunens Internet
8.1.1	När du använder internet genom kommunens nätverk ska du göra så med ett gott omdöme och aldrig medvetet besöka sidor som du misstänker kan vara skadliga
8.1.2	Det är inte tillåtet att från kommunens nätverk titta eller lyssna på material av pornografisk eller rasistisk karaktär som finns tillgängligt på internet. Förbudet gäller också material

	Regler för användandet E-post
9.1	Du är skyldig att rapportera alla incidenter kopplat till informationssäkerhet.
9.2	Om du misstänker att någon använt din användaridentitet eller att din dator infekterats med skadlig kod eller virus eller någon annan typ av incident som påverkar informationssäkerheten ska du: • Notera när du senast var inne i informationssystemet. • Notera när du upptäckte incidenten. • Notera om någon sekretessbelagd information, personuppgifter eller för verksamheten annan känslig information finns lagrad i din dator eller motsvarande • Omedelbart anmäla förhållandet till IT-enheten, din chef och kommunens Dataskyddsombud • Dokumentera alla iakttagelser i samband med upptäckten. • Samverka vid incidentanmälan till Datainspektionen och andra myndigheter

10. Virus och annan skadlig kod

Kommunen har programvaror för övervakning och kontroll av skadlig kod både på datorerna och i nätverket. Anti-virusprogramvara finns installerat på samtliga datorer och dessa uppdateras automatiskt. Läsplattornas anti-virusprogramvara finns inbyggt och uppdateras samtidigt med nya versioner av operativsystemet i läsplattan.

Kommunen kan ändå inte garantera att du inte drabbas av effekter av skadliga programvaror. Läsplattor, digitala kameror, smarta mobiltelefoner, USB-minnen m.m. kan vid oaktsamhet bli virusbärare eftersom du kan mellanlagra information mellan olika datorer i dessa. Den dator du ansluter sådan kringutrustning till måste ha ett uppdaterat anti-virusprogram.

	Virus och skadlig kod
10.1	Om du misstänker att din dator innehåller virus eller annan skadlig kod ska du, utöver vad som tidigare specificerats för incidenter, vidta följande åtgärder: • dra ut nätverkskabeln eller koppla ifrån det trådlösa nätverket men låta datorn vara på, och • omedelbart anmäla det som en informationssäkerhetsincident till IT-enheten.