NORDANSTIGS KOMMUN

Riktlinjer för informationssäkerhet

Dokumentnamn Riktlinjer för informationssäkerhet.docx			**Reviderad** datum 2020-10-06 - - - - - - - - - - - - - - - - - -
Dokumentansvarig Morgan Norell	**Fastställd av** Kommunstyrelsen § 300, 2019-12-03 Reviderad 2020-10-06 KS § 161		
Diarienummer 2019-000342	**Original** datum **2019-08-09**	**Giltig** till och med **2023-12-31**	

Informationssäkerhet

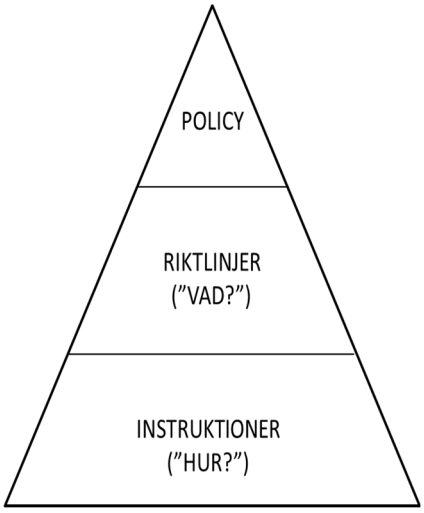
Information är en av kommunens viktigaste tillgångar och hanteringen av den är en mycket viktig del i arbetet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i. Informationssäkerheten omfattar kommunens alla informationstillgångar.

Struktur

I *Informationssäkerhetspolicyn* fastställs synen på informationssäkerhet, övergripande mål och organisationens intention med informationssäkerhetsarbetet.

I detta dokument, *Riktlinjer för informationssäkerhet*, beskrivs vad som måste etableras för att uppfylla informationssäkerhetspolicyn.

Utifrån detta upprättas sedan instruktioner, som detaljerat redogör för hur exempelvis rutiner och säkerhetslösningar ska utformas och tillämpas, för att informationssäkerhetspolicyn och riktlinjerna ska följas.



Sammantaget är detta kommunens regelverk för informationssäkerhet.

Hantering av tillgångar

Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är informationsägare och i förekommande fall objektsägare.

Alla verksamheter och system är utsatta för risker. Risk- och sårbarhetsanalysen ska identifiera tänkbara störningar, allvarliga händelser samt extraordinära händelser. Arbetet syftar till att skapa robusta system samt identifiera och analysera skyddsvärda informationstillgångar. Arbetet ska fokusera på förebyggande insatser och konkreta skyddsåtgärder för människor, egendom och miljö.

Klassificering av information

Klassificering av information är en grundläggande aktivitet för att alla informations-tillgångar och resurser ges nödvändigt skydd. Det är informationen som är skyddsobjektet, dvs. det som ska skyddas. Dock kan överklassificering medföra onödiga åtgärder med ytterligare kostnader till följd.

Informationen ska klassificeras utifrån den funktion och betydelse för verksamheten som den har och de konsekvenser det medför om informationen skulle hanteras felaktigt, försvinna, komma i orätta händer m.m.

Vid klassificering av information ska det bedömas vilken negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ får inom följande fyra kravområden:

- Konfidentialitet - att förhindra eller försvåra för obehöriga att få tillgång till information, informationen åtkomstbegränsas

- Riktighet - att den information som produceras och bearbetas är tillförlitlig, aktuell och fullständig

- Tillgänglighet - att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet

- Spårbarhet – att identifiera och autentisera användare, samt loggning av relevanta händelser

Vid bedömning används följande fem konsekvensnivåer:

- Synnerligen allvarlig – skada för rikets säkerhet som inte endast är ringa

- Allvarlig – informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, eller fara för liv och hälsa

- Betydande – tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, eller förlust av skapat förtroende

- Måttlig – minskad förmåga att genomföra verksamhetens uppdrag, effektiviteten är påvisbart reducerad

- Försumbar – ingen eller försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation

Personalresurser och säkerhet

Alla anställda, uppdragstagare och utomstående användare ska förstå sitt ansvar. Det ska säkerställas att dessa är lämpliga för de roller de anses ha i syfte att minska risken för stöld, bedrägeri eller missbruk av resurser. Det ska också säkerställas att de är medvetna om hot och problem som rör informationssäkerhet samt är rustade för att följa kommunens regelverk för informationssäkerhet när de utför sitt normala arbete och för att minska risken för mänskliga fel.

När anställda, uppdragstagare och utomstående användare lämnar kommunen eller ändrar anställningsförhållande ska det ske på ett ordnat sätt.

Fysisk och miljörelaterad säkerhet

Nivån på det fysiska skyddet ska stå i proportion till resultatet av informations-klassificeringen och de i återkommande riskanalyser.

Utrustning ska skyddas mot förlust, skada, stöld eller skadlig påverkan på tillgångar och avbrott i kommunens verksamhet.

Kommunikation och drift

Kommunen ska ha en korrekt och säker drift av IT-miljö, nätverk och tillhörande infrastruktur så att informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet upprätthålls.

Risken för systemfel ska minimeras och systemintegriteten för programvara och riktighet i information ska säkerställas genom tydliga förvaltningsmodeller och adekvata tekniska skydd mot exempelvis skadlig kod.

Informationens och IT-miljöns riktighet respektive systemintegritet och tillgänglighet ska bevaras genom väl utvecklade rutiner för säkerhetskopiering och återläsning.

De ska finnas tydliga instruktioner som hindrar att information på flyttbart och avvecklat media avslöjas.

Kritiska och säkerhetsrelevanta händelser ska vara spårbara genom automatiska loggningsfunktioner som skyddas mot manipulation och obehörig åtkomst.

Åtkomst till system och information ska styras utifrån verksamhetens behov och säkerhetskrav. Den som har behov av tillgång till viss information för att kunna utföra sina arbetsuppgifter ska tilldelas åtkomsträttigheter. All åtkomst ska vara behovsbaserad utifrån ansvars- och arbetsområde.

Alla administratörer ska ha individuella användaridentiteter. Användare ska hantera sina inloggningsuppgifter på ett sätt så att obehörig åtkomst undviks.

Anskaffning, utveckling, underhåll och avveckling av system

Alla system inom kommun ska ha tillräckliga skydd så att informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet upprätthålls.

Systemen ska utformas så att fel, obehörig förändring eller missbruk förhindras genom exempelvis validering av in- och utdata och andra adekvata kontroller.

Risker med publicerade sårbarheter ska hanteras.

Vid anskaffning ska gallring och arkivering vägas in och beaktas särskilt för att stötta informationens hela livscykel. Plan för avveckling ska finnas redan vid anskaffning av ett system. Krav på gallring och arkivering ska beaktas vid avveckling. Uppgifter som gallras ska förstöras på ett sådant sätt att uppgifterna inte kan återskapas eller komma i orätta händer.

Hantering av informationssäkerhetsincidenter

Incidenter och säkerhetsmässiga svagheter ska, utan dröjsmål, rapporteras och korrigerande åtgärder ska vidtas i rätt tid.

Kontinuitetsplanering

Kontinuitetsplaner ska upprättas och införas för de kritiska verksamhetsprocesserna för att säkerställa att identifierade viktiga funktioner kan återställas inom rimlig tid och att verksamheten har manuella rutiner för tiden under återuppbyggnadsarbetet.

Kontinuitetsplanen ska baseras på analys av konsekvenserna av störningar, allvarliga händelser, och extraordinära händelser med hänsyn till dess inverkan på verksamheten.

Efterlevnad

Chefer ska säkerställa att alla säkerhetsrutiner inom deras respektive ansvarsområden utförs korrekt för att upprätthålla informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Vitala system och vitala delar i IT-miljö, nätverk och tillhörande infrastruktur ska regelbundet kontrolleras så att informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet upprätthålls.

Extern revision ska utföras på ett sådant sätt att informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet inte påverkas.

Ytterligare information

För vidare information se respektive instruktion