SÅ HÄR GÖR VI I NACKA
Så här arbetar vi med informationssäkerhet i Nacka kommun

Diarienummer	Fastställd/senast uppdaterad	Beslutsinstans	Ansvarigt politiskt organ	Ansvarig processägare
KFKS 2013/754-001	Ange datum.	Stadsdirektör	Kommunstyrelsen	Stabs- och säkerhetsdirektör
Så här gör vi i Nacka	Så här arbetar vi med informationssäkerhet i Nacka kommun			

Så här arbetar vi med informationssäkerhet i Nacka kommun

Dokumentets syfte

Beskriver vad vi gör i Nacka rörande informationssäkerhetsarbetet.

Dokumentet gäller för

Alla chefer och medarbetare i Nacka kommun

Informationstillgångar avser all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i. Arbetet med informationssäkerheten är en integrerad del i verksamheten.

Utgångspunkter

I arbetet med informationssäkerhet ska följande krav säkerställs:

- Tillgänglighet - att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet
- Riktighet - att informationen är tillförlitlig, korrekt och fullständig
- Konfidentialitet - att informationen kan åtkomstbegränsas om så krävs
- Spårbarhet - att specifika aktiviteter som rör informationen ska kunna spåras

Samtliga anställda och externa aktörer ska ha kännedom om Nacka kommuns regelverk kring informationssäkerhet samt följa dessa. Alla som hanterar informationstillgångar har ett ansvar att informationssäkerheten upprätthålls. Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

Samverkan med konsulter, externa leverantörer och entreprenörer ska regleras genom avtal. Vid behov av åtkomst till informationsresurser bör en riskbedömning göras för att identifiera ytterligare krav på säkerhet.

Hantering av tillgångar

Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är informationsägare eller systemägare. 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 före-byggande insatser och konkreta skyddsåtgärder för människor, egendom och miljö.

Klassificering av information

Klassificering av information är en grundläggande aktivitet för att informationstillgångar 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 etc. Vid klassificering av information ska det bedömas i vilken grad förlust av konfidentialitet, riktighet, tillgänglighet eller spårbarhet hos information innebär negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ. Vid bedömning används en fyrgradig skala.

1. Försumbar skada
2. Måttlig skada
3. Betydande skada
4. Allvarlig skada

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 informationsklassificeringen och 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 rutiner som hindrar att information på flyttbar och avvecklad 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 och underhåll av system

Alla system inom kommun ska ha erforderliga 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.

Hantering av informationssäkerhetsincidenter

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

Kontinuitetsplanering för verksamheten

Kontinuitetsplaner ska upprättas och införas 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

Kommunen ska säkerställa att överträdelser av lagar, författningar eller avtalsförpliktelser, samt andra säkerhetskrav inte sker. Chefer inom kommunen ska se till att alla säkerhetsrutiner inom deras respektive ansvarsområde utförs korrekt för att uppnå efterlevnad av kommunens informationssäkerhetsregelverk.

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.