Handläggare	Vårt diarienummer	Datum	Sidan 1(8)
Jonas Åström	KS2016/222	2016-04-29	

VISION
STRATEGI
REGLEMENTE
PROGRAM
POLICY
PLAN
» RIKTLINJE
REGEL

Sandvikens kommuns

Riktlinjer för informationssäkerhet

Sandvikens kommuns styrdokument

» Aktiverande

VISION – övergripande måldokument, beskriver den framtid organisationen strävar mot

STRATEGI – avgörande vägval för att nå målen för Sandvikens kommun

PROGRAM – verksamheter och metoder i riktning mot målen

PLAN – lagstadgad benämning och styrdokument

» Normerande

REGLEMENTE – ansvarsområde och arbetsformer

POLICY – Sandvikens kommuns förhållningssätt, viljeinriktning samt principer inom ett område

RIKTLINJE – rekommenderade sätt att agera

REGEL– absoluta gränser och ska-krav

Styrdokumentets data

Fastställt av: Kommunfullmäktige

Datum och paragraf: 2016-06-13, §119

Diarienummer: KS2016/222

För revidering ansvarar:

För uppföljning och tidplan för denna ansvarar:

Dokumentet gäller för: Kommunkoncernen

Dokumentet gäller från och med: 2016-07-01

Dokumentet gäller till och med: tills vidare

Dokumentansvarig: Informationssäkerhetssamordnare

Rätt att göra revideringar under löptiden: KS

Revidering av styrdokumentet

Rätt att revidera ges på delegation från beslutande organ. I beslutet ska det framgå att delegationen t.ex. gäller administrativa förändringar.

Orsak till revidering:

Förändring i dokumentet:

Beslut av:

Beslutsdatum:

Diarienumm

Innehåll

1 Informationssäkerhet

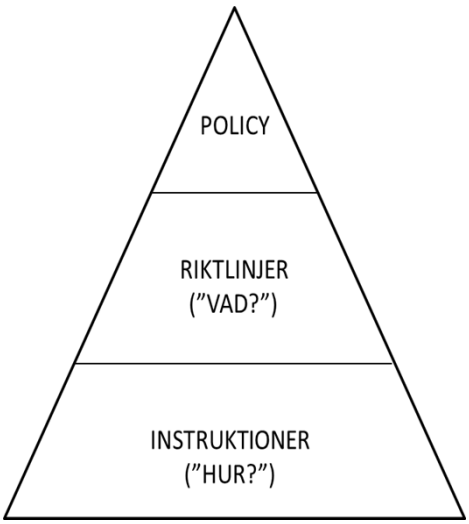
Information är en av kommunens viktigaste tillgångar och hanteringen av den är en mycket viktig del i arbetet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i. Informationssäkerheten omfattar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

2 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.

3 Hantering av tillgångar

Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är informationsägare och i förekommande fall 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 förebyggande insatser och konkreta skyddsåtgärder för människor, egendom och miljö.

4 Klassificering av information

Klassificering av information är en grundläggande aktivitet för att alla informationstillgångar och resurser ges nödvändigt skydd. Det är informa-

tionen 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.

Klassificering av information ska ske inom följande fyra kravområden:

- Konfidentialitet – att informationen kan åtkomstbegränsas (benämndes tidigare sekretess men standarden har ändrats för att inte förväxla begreppet med sekretess i juridisk mening)
- Riktighet – att informationen ska vara tillförlitlig, korrekt och fullständig
- Tillgänglighet – att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet
- Spårbarhet – att specifika aktiviteter som rör informationen kan spåras

Vid bedömning används följande fyra konsekvensnivåer:

- Allvarlig skada – t.ex. massiv informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, samt fara för liv och hälsa
- Betydande skada – t.ex. tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, samt förlust av skapat förtroende
- Måttlig skada – t.ex. minskad förmåga att genomföra verksamhetens uppgifter, men effektiviteten är påvisbart reducerad
- Försumbar skada

5 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.

6 Fysisk och miljörelaterad säkerhet

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

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

7 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.

8 Lagring av dokument

Integritetskänslig eller sekretessinformation ska i första hand lagras i ett befintligt verksamhetssystem som är säkerhetsmässigt godkänt och i andra hand lagras på någon av enheterna H: eller G: i nätverket. Vid lagring på G: måste behörigheten till mappen och dokumentet särskilt anges

Information, som är offentlig eller som inte är integritetskänslig får lagras i molnet (OneDrive) m. fl. verktyg i Office 365. Vad som anses vara integritetskänsligt eller som omfattas av sekretess och/eller tystnadsplikt innehåll kan du få hjälp av din chef att definiera

Lagring av filer på datorns skrivbord eller på användarens lokala disk ska undvikas då dessa lagringsplatser inte säkerhetskopieras. Dokument som

sparats på dessa platser kan försvinna vid t ex ett datorhaveri eller vid en ominstallation av datorn.

9 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.

10 Hantering av informationssäkerhetsincidenter

Incidenter och säkerhetsmässiga svagheter ska utan dröjsmål rapporteras till Servicedesk på IT-kontoret och ansvarig för Informationssäkerheten i kommunen. Korrigerande åtgärder ska vidtas snarast möjligt.

11 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.

12 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.

13 Ytterligare information

Dessa riktlinjer är utarbetad helt i enlighet med de normativa kraven i SS-ISO/IEC 27001:2013.

För vidare information se respektive instruktion.