Informationssäkerhetspolicy för Sundbybergs stad

Dokumenttyp: policy
Fastställd av: Kommunfullmäktige 30 oktober 2017, § 367
Status: Godkänd
Giltighetstid: Tillsvidare

Diarienummer	KS-0726/2015
Tidpunkt för fastställande	30 oktober 2017, § 367
Dokumentägare	Kommunstyrelsen
Dokumentansvarig	Stadsdirektör
Intervall för aktualitetsprövning	Årligen
Tidpunkt för senaste revidering	
Relaterade styrdokument	-

Informationssäkerhetspolicy för Sundbyberg stad

Denna policy utgör grunden för en säker hantering av information inom Sundbybergs stad, policyn omfattar även hela kommunkoncernen.

Tillgången till information är en förutsättning för koncernens möjligheter att fullgöra sina åtaganden. Därmed är information en viktig tillgång och en av koncernens mest strategiska resurs, som måste behandlas och skyddas på ett tillfredställande sätt, samtidigt som tillgången till information och öppenhet inom koncernen ska vara så stor som möjligt. Störningar i tillgången till information kan vara kritisk och felaktig information kan leda till allvarliga konsekvenser.

Informationssäkerhet är en integrerad del av koncernens verksamhet och dess syfte omfattar punkterna nedan.

- att informationen kan åtkomst begränsas
- att informationen ska vara tillförlitlig, korrekt och fullständig
- att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet
- att specifika aktiviteter som rör informationen kan spåras

Definition

Med informationssäkerhet avses i denna policy all information som hanteras inom koncernen, oavsett i vilken form den återfinns eller behandlas – digitalt, på papper eller i konversation och oberoende i vilken form eller miljö den förekommer. Informationssäkerhet avser att ge rätt skydd till den information som behandlas eller lagras. Informationssäkerhetsarbetets mål definieras utifrån dessa fyra aspekter:

- **Konfidentialitet** – att innehållet i informationsobjekt inte får göras tillgängligt eller avslöjas för obehöriga
- **Riktighet** – att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning
- **Tillgänglighet** – informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid
- **Spårbarhet** – det ska vara möjligt att i efterhand härleda hur uppgifter har behandlats och av vem

Syfte

Syftet med informationssäkerhetsarbetet är att skydda koncernens verksamheter mot avbrott i informationsflödet och minimera risken för att informationen används så att den skadar koncernen, dess medarbetare, kunder och invånare, eller tredjeman. För koncernens informationsarbete gäller:

- att all personal har tillräckliga kunskaper om informationssäkerhet i förhållande till sina arbetsuppgifter
- att informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- att informationssäkerhetsarbetet ska bedrivas med tyngdpunkt på risk- och sårbarhetsanalyser samt förebyggande aktiviteter

Struktur

Informationssäkerhetsarbetet tar sin utgångspunkt från standarden ISO/IEC 27001, verksamhetens krav, gällande lagar och förordningar. Vidare ska De 16 principerna för samverkan inom region Stockholm[1] följas.

Policyn konkretiseras via riktlinjer och anvisningar, arkivreglemente, arkivbeskrivning och dokumenthanteringsplaner. Riktlinjerna fastställs av koncernledningen.

Roller och ansvar

Respektive bolagsstyrelse och nämnd är ansvarig för att upprätthålla informationssäkerheten inom sina respektive verksamheter. Kommunstyrelsen ansvarar för att leda, samordna och granska hela koncernens informationssäkerhetsarbete.

Bolagsstyrelser och nämnderna ska

- genom verksamhetsrutiner, granskningar, informationsklassning, riskhantering och kontinuitetsplanering minimera och förebygga störningar i verksamheten
- tillförsäkra att all informationsbehandling följer koncernens regelverk för informationssäkerhet, standarder och att de skyddsåtgärder som fordras implementeras
- minimera risken för avsiktlig eller oavsiktlig överträdelse av lagregler, avtalsförpliktelser m.m.
- tillse att informationssäkerhetsaspekter beaktas vid utveckling, anskaffning, förvaltning och avveckling av informationsbärare samt informationstillgångar

Revidering och uppföljning

Koncernledningen ska löpande informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet.

---

[1] DNR 00186/2010-530 Beslutade i kommunstyrelsen den 1 juni 2010