HELSINGBORG

Informationssäkerhets-policy

PROGRAM PLAN **POLICY** RIKTLINJER

Helsingborgs stads styrdokument

Aktiverande
syftar till förändring och utveckling

PROGRAM – anger långsiktiga ambitioner och viljeinriktningar
PLAN – anger konkreta åtgärder, tidsramar och ansvar

Normerande
reglerar befintlig verksamhet och vårt förhållningssätt till en given situation

POLICY – anger principer och vägledning
RIKTLINJER – anger absoluta gränser och ska-krav

Beslutat av: Kommunfullmäktige
Datum: 16 december 2009, § 191
Dokumentet gäller för: Alla nämnder och förvaltningar
Dokumentansvarig: Avdelningen för strategisk samhällsutveckling vid stadsledningsförvaltningen

HELSINGBORG

Innehållsförteckning

Informationssäkerhet

Inledning

Denna policy anger riktlinjerna för informationssäkerheten inom Helsingborg stad. Policyn omfattar all information och informationsbehandling i Helsingborg stad, dess nämnder och förvaltningar och gäller för anställda, förtroendevalda och stadens samarbetspartners.

Information som stadens verksamhet behöver för att lösa sina uppgifter är många gånger både känslig och kritisk till sin natur och finns i alla förvaltningar och beslutande organ. Helsingborgs stads invånare förväntar sig att förvaltningar och nämnder behandlar information på ett betryggande sätt och att man har tillgång till nödvändig information även i händelse av krissituationer.

Staden informationsresurser är därför av strategisk betydelse och egenskaperna sekretess, riktighet, tillgänglighet och spårbarhet måste beaktas.

Informationssäkerhet inom Helsingborg stad definieras som:

- att rätt information är tillgänglig för rätt person, vid rätt tid
- att känslig information undanhålls obehöriga
- att information är och förblir riktig
- att åtkomst till, och förändring av, information är spårbar

Arbetet med informationssäkerhet i Helsingborgs stad utgår ifrån relevanta lagar, förordningar och föreskrifter, samt stadens egna krav och avtal med externa parter.

Informationssäkerhetspolicyn utgör stadens bindande styrdokument och redovisar kommunfullmäktiges viljeinriktning och målsättning för säker informationsbehandling. Vid behov kan policyn konkretiseras genom utfärdande av anvisningar och instruktioner.

Definitioner

Med informationssäkerhet avses förmågan att upprätthålla önskad sekretess, riktighet och tillgänglighet vid hantering av information. Begreppet är omfattande och rör information i alla dess former, både i pappersform och elektroniskt hanterad.

Sekretess är skyddsmålet att inte obehöriga kan ta del av informationen.

Riktighet att informationen inte förändras eller förstörs på ett obehörigt sätt.

Tillgänglighet att behöriga får tillgång till informationen på det sätt och vid den tidpunkt som önskas.

Spårbarhet att kunna avgöra händelseförlopp och förändringar i information.

Informationssystem är ett gemensamt begrepp på system som används för att skapa, förmedla eller bearbeta information.

Mål och metod

Information är i en av de viktigaste tillgångarna och en förutsättning för att verksamhet ska kunna bedrivas. Om den inte hanteras på rätt sätt kan även Helsingborgs stads goda namn och rykte äventyras.

Det övergripande målet med Helsingborgs stads informationssäkerhet är att skapa kontinuitet i stadens verksamheter genom att skydda och säkerställa informationstillgångarna så att rätt information är tillgänglig för rätt person i rätt tid på ett spårbart sätt.

Helsingborgs stad har därutöver följande mål med informationssäkerhetsarbetet:

- Känslig information skall undanhållas obehöriga.
- Kritiska informationssystem och infrastruktur för tele- och datakommunikation skall ha hög tillgänglighet.
- Kritiska informationssystem och infrastruktur för tele- och datakommunikation skall ha skyddsfunktioner motsvarande hotbilden.

För att nå målen skall:

- stadens informationstillgångar fortlöpande identifieras, klassificeras och relevanta hot värderas och hanteras
- alla informationssystem ha en systemägare och vara väl dokumenterade
- riskanalyser (innefattande hot- och sårbarhetsanalyser) genomföras regelbundet för kritiska kommunala funktioner (tjänster)
- staden kontinuerligt arbeta med att informera och utbilda anställda i informationssäkerhet
- förebyggande åtgärder prioriteras

Organisation och ansvar

Kommunfullmäktige fastställer informationssäkerhetspolicyn. Kommunstyrelsen har det övergripande ansvaret för informationssäkerheten.

Kommunstyrelsen har också det övergripande ansvaret för att den interna kontrollen fungerar tillfredställande samt för att informationssäkerhetspolicyn årligen granskas och vid behov revideras.

Stadsdirektören fastställer, på delegation av kommunstyrelsen, kommunövergripande anvisningar.

Varje nämnd är ansvarig för informationssäkerheten inom sitt/sina verksamhetsområden. Respektive förvaltningschef ansvarar för att informationssäkerhetsarbetet bedrivs i linje med fastställd informationssäkerhetspolicy.

Chefer på alla nivåer ansvarar för att informationssäkerheten efterlevs enligt gällande policy och anvisningar inom sitt respektive ansvarsområde.

Varje medarbetare ansvarar för att tillämpa gällande policy och anvisningar inom det egna ansvarsområdet. Varje medarbetare förväntas också vara uppmärksam på och rapportera händelser som kan påverka säkerheten och aktivt verka för att förbättra säkerheten inom sin verksamhet.

Stadens revisorer utför kontroll av informationssäkerheten inom ramen för sin förvaltningsrevision.

Informationssäkerhetsarbetet i staden samordnas av avdelningen för Trygghet och säkerhet, Stadsledningsförvaltningen. I deras uppgift ingår även att utvärdera informationssäkerhetsarbetet, ge råd samt föreslå åtgärder.

Revidering och godkännande

Denna policy skall löpande följas upp av avdelningen för Trygghet och säkerhet, Stadsledningsförvaltningen, för att säkerställa att den hålls aktuell i förhållande till omvärlden och vid behov revideras. Förändringar av annan karaktär än redaktionella skall beslutas av kommunfullmäktige.

Vägledande dokument

Basnivå för informationssäkerhet, BITS, från Krisberedskapsmyndigheten
Ledningssystem för informationssäkerhet, ISO 27000-serien

Giltighet

Organisationsnamn är reviderade den 21 maj 2012. DNR KS 406/2012.