IT-SÄKERHETSPOLICY

Inledning

Denna informationssäkerhetspolicy anger Halmstads kommuns mål för informationssäkerheten samt riktlinjer för hur dessa ska uppnås. Informationssäkerhetspolicyn kommer att fördjupas i en säkerhetsplan som sedan kompletteras med systemsäkerhetsplaner för de enskilda datasystemen. En översikt över alla styrande dokument återfinns i bilaga 1.

Det övergripande ansvaret för Halmstads kommuns datasystem åvilar nämnder/styrelser. Det operativa ansvaret för att varje enskilt datasystem uppfyller krav på säkerheten följer linjeorganisationen.

Definition

Med informationssäkerhet (i detta dokument förkortat IT-säkerhet) avses skyddet av konfidentialitet, informationskvalitet och tillgänglighet hos information som hanteras av datoriserade informationssystem samt även skyddet av själva systemet.

Med verksamhets-/datasystem avses de datasystem som är nödvändiga för en fungerande verksamhet.

Omfattning

Denna policy omfattar samtliga Halmstads kommuns nämnder, styrelser samt helägda bolag.

Mål för IT-säkerhetsarbetet

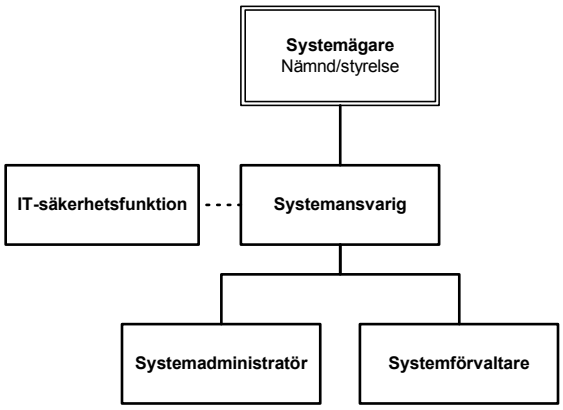
Målen för Halmstads kommuns IT-säkerhetsarbete är att:

- Samtliga datasystem inom Halmstads kommun skall uppnå grundsäkerhet enligt FA22.
- För varje datasystem skall, utöver grundsäkerheten, verksamhetsrelaterade krav och hotrelaterade krav fastställas i en systemsäkerhetsplan.
- Säkerhetsåtgärder i datasystemen utformas och förvaltas på ett sådant sätt att kraven uppfylls,
- En årlig uppföljning och kontroll av IT-säkerheten skall ske, bl.a. som underlag för verksamhetsplanering.
- Varje datasystem skall formellt driftgodkännas samt
- Halmstads kommun skall kunna utföra sina arbetsuppgifter på ett tillfredsställande sätt även under höjd beredskap.

Ledning och ansvar för IT-säkerheten

En fastställd ansvarsfördelning för datasystemsäkerheten är en förutsättning för att Halmstads kommun ska kunna leva upp till sin IT-säkerhetspolicy. Säkerhetsansvaret följer den normala linjeorganisationen. Var och en, som är ansvarig för någon del av verksamheten, ansvarar också för IT-säkerheten inom sitt område.

Med IT-säkerhetsorganisation avses den funktionella organisationen som inom Halmstads kommun ansvarar för att informationssäkerheten baseras på ett kombinerat risk- och lönsamhetstänkande och att åtgärder bestäms utifrån interna och externa krav.



Figur 1 - Organisatoriska roller

Systemägare

Är den nämnd/styrelse inom vars verksamhetsområde ett datasystem används, förvaltas och administreras.

Systemansvarig

Systemansvarig utses av systemägare och är dess företrädare. Har nämnden/styrelsen inte utsett en systemansvarig är förvaltnings-/bolagschefen dess företrädare.

Systemförvaltare

Systemförvaltaren har det övergripande ansvaret för att de olika datasystemens tekniska delar fungerar.

Systemadministratör

Systemadministratören ansvarar för, tillsammans med systemförvaltare, att den dagliga driften upprätthålls enligt överenskommelse med systemansvarig.

IT-säkerhetsfunktion

IT-säkerhetsfunktionen understödjer arbetet med att uppnå säkerhetsplanens mål. Detta kan innebära aktivt deltagande i projekt, etablerandet av interna och externa kontaktnät, utvärdering och deltagande i diskussioner kring metoder, plattformar, applikationer eller datasystem.

Lagar och andra regelverk

Ramarna för Halmstads kommuns IT-säkerhetsarbete sätts utifrån lagar och andra regelverk. Dessa anger bland annat villkoren för de övergripande säkerhetskrav som ställs på verksamheten och därmed även på hanteringen av information i datasystem.

Detta omfattar bland annat:

- Skyddet för den personliga integriteten
- Att sekretessbelagd information skall skyddas mot otillbörlig åtkomst, med iakttagande av offentlighetsprincipen.
- Olika intressenters krav på korrekt information och allmänhetens lagliga rätt till insyn i offentliga handlingar.
- Speciallagstiftning.

IT-säkerhetsarbetet

IT-säkerhetsarbetet inom Halmstads kommun skall följa den process i säkerhetsarbetet som är baserad på FA22.

FA22 är uppbyggt så att det indirekt anger en logisk arbetsprocess för IT-säkerhetsarbetet, se bilaga 1 - Styrande dokument.

Driftgodkännande

Alla system inom Halmstads kommun skall ha en sådan säkerhet att de kan driftgodkännas. Säkerhetsarbetet skall för varje system bedrivas så att ett driftgodkännande kan beslutas senast 2003-06-30. De åtgärder som då eventuellt återstår skall vara dokumenterade och det skall finnas en tidsplan för när de skall vara genomförda.

Styrande dokument

De dokument som är styrande för IT-säkerhetsarbetet är följande:

Dokument	Nivå	Innehåll	Upprättas av	Fastställs av
IT-säkerhetspolicy	Generell	Mål för IT-säkerhetsarbetet vid Halmstads kommun och övergripande riktlinjer	IT-säkerhetsfunktion	Kommunfullmäktige
Säkerhetsplan	Generell	Riktlinjer för IT-säkerhet i Halmstads kommuns nätverk.	IT-säkerhetsfunktion	Systemägare
Systemsäkerhetsplan	Per system	Mål för IT-säkerheten för enskilt datasystem	Systemansvarig	Systemägare
Säkerhetsinstruktion	Generell	Övergripande säkerhetsregler för infrastrukturen	IT-säkerhetsfunktion	Kommunstyrelsen
Säkerhetsinstruktion	Per system	Säkerhetsregler för enskilt datasystem	Systemansvarig	Systemägare
Säkerhetsinstruktion	För användare	Säkerhetsregler för användare	IT-säkerhetsfunktion	Systemägare
Beredskapsplan	Generell	Plan för höjd beredskap	IT-säkerhetsfunktion	Kommunstyrelsen
Avbrottsplan	Per system	Plan för avbrott	Systemansvarig	Systemägare
Katastrofplan	Per system	Plan för katastrof	Systemansvarig	Systemägare
Driftgodkännande	Per system	Formellt driftgodkännande av datasystem	IT-säkerhetsfunktion	Systemägare

Tid- och kostnadsuppskattning för systemsäkerhetsplan

För varje verksamhetssystem ska en systemsäkerhetsplan upprättas. Detta kommer att genomdrivas i projektform på respektive förvaltning. Handledning kommer att ges från Stadskontoret.

Tidplan

Tidplanen för projekten kan se lite olika ut beroende på systemens storlek och förekomsten av befintlig dokumentation. Projektens löptid beräknas vara ca 3 månader för att inte vara för stor belastning för den ordinarie verksamheten.

Kostnader av systemsäkerhetsplan

För att upprätta systemsäkerhetsplaner för de olika verksamhetssystemen krävs insatser i form av mantimmar. Antalet timmar kan variera beroende på hur mycket dokumentation som redan finns och hur **omfattande** verksamhetssystemen är. En ungefärlig uppskattning på timåtgången (antalet mantimmar) redovisas i tabellen nedan.

Inledning	Genomgång av FA22	4 timmar
Fas 1 - Dokumentation	Verksamhetssbeskrivning	8 timmar
	Informationsbeskrivning	8 timmar
	Organisation och ansvar	8 timmar
	Genomgång	8 timmar
Fas 2 - Grundsäkerhet	HK riktlinjer	8 timmar
Fas 3 - Säkerhetsklassning	Säkerhetskrav	8 timmar
Fas 4 - Åtgärdsplan	Grundsäkerheten	16 timmar
	Tilläggskrav	16 timmar
Fas 5 - Tidsplan	Tidsplanering	16 timmar
Fas 6 - Avbrottsplan	Alternativa rutiner	16 timmar
	Återstartsrutiner	16 timmar
	Handlingsberedskap	16 timmar
Fas 7 - Katastrofplan	Reservrutiner	16 timmar
	Alternativt driftställe	8 timmar
	Förebyggande arbete	16 timmar
Beräknad tidsåtgång		**188 timmar**

Kostnader för åtgärder

De eventuella åtgärder som behövs göras för respektive verksamhetssystem ska dokumenteras i en åtgärdsplan, och där även en tidsplan för när åtgärderna ska vara uppfyllda. På detta sätt ges möjligheten för förvaltningarna att budgetera för eventuella framtida investeringar som krävs.