IT-säkerhetspolicy

Höörs kommun

Fastställd av KF 2005-02-16

Revisionsinformation

Datum	Åtgärd	Ansvarig	Version
2004-11-19	3.4 Ändrat första meningen förvaltningen -> verksamheten 3.6 Lagt till att IT-enheten tillsammans med säkerhetsfunktionen ansvarar för årlig revidering av policyn 3.8 Se 3.6	PGR	2.0
2004-12-07	3.7 Ändrat formulering	PGR	2.0
2005-01-19	5. Tillägg om rapportering kring IT-säkerhetsarbetet	PGR	2.0
2005-02-14	Ändrat IT-avdelningen -> IT-enheten	PGR	Final 3.0

Innehållsförteckning

1 Inledning 4
2 Mål för IT-säkerhetsarbetet 4
3 Organisation kring IT-säkerhet 4
3.1 Allmänt 4
3.2 Ledning och ansvar för IT-säkerhet 4
3.3 Systemägare 5
3.4 Verksamhetsansvariga 5
3.5 Systemförvaltare 5
3.6 IT-enheten 6
3.7 Användare 7
3.8 IT-säkerhetsfunktion 7
4 Lagar och andra regelverk 7
5 IT-säkerhetsarbetet inom Höör kommun 7
6 Driftgodkännande 8
BILAGA 1 STYRANDE DOKUMENT – ÖVERSIKT 9

1 Inledning

Denna IT-säkerhetspolicy beskriver övergripande arbetet med- och ansvar kring IT-säkerhet i Höörs Kommun. Med utgångspunkt i policyn kommer regler, riktlinjer och handlingsplaner att tas fram. En översikt över samtliga relaterade dokument återfinns i bilaga1.

Höörs kommuns IT-säkerhet skall följa den basnivå som definieras av BITS[1].

Det övergripande ansvaret för Höörs kommuns datasystem ligger på kommunstyrelsen. Det operativa ansvaret för att varje enskilt datasystem uppfyller verksamhetens krav på säkerhet följer linjeorganisationen.

2 Mål för IT-säkerhetsarbetet

Målen för Höörs kommuns IT-säkerhetsarbete är att:

- IT-verksamheten skall vara säker. Informationen skall vara skyddad mot otillbörlig åtkomst.
- Informationen skall vara tillförlitlig. Felaktigheter som skadar verksamheten eller enskilda får inte förekomma
- Verksamheten skall kunna utföra sina uppgifter på ett tillfredställande sätt vid extraordinära händelser i fred samt under höjd beredskap.

3 Organisation kring IT-säkerhet

3.1 Allmänt

För att uppnå målen krävs en effektiv samverkan mellan människor och teknik. Dessutom gäller att:

- Grundsäkerheten, som definieras av BITS uppnås
- Gällande lagar, föreskrifter och författningar följs.
- All personal har kunskap om Höörs kommuns riktlinjer för IT-användningen
- Säkerhetsgranskning av samtliga förvaltningsspecifika system fastställs i en systemsäkerhetsplan.
- Samtliga nya system formellt driftgodkänns innan inköp och driftstart.
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för IT-verksamheten.
- Löpande analysera hotbilden för varje enskilt datasystem
- IT-säkerhetsarbetet följs upp och IT-säkerhetspolicyn ses över varje år.

3.2 Ledning och ansvar för IT-säkerhet

En fastställd ansvarsfördelning för datasystemsäkerheten är en avgörande förutsättning för att Höörs kommun skall 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.

Nedan redovisas ansvarsfördelningen för olika rollinnehavare. I många fall kan samma person inneha flera av dessa roller.

[1] Basnivå för IT säkerhet – Krisberedskapsmyndigheten 2002:3

3.3 Systemägare

Systemägare är nämnden, denna har det övergripande ansvaret för att datasystemet förvaltas på ett för verksamheten bästa sätt. Systemägaren fattar de avgörande besluten om datasystemets utveckling eller avveckling inom ramen för resurstilldelningen för sin verksamhet.

Systemägaren har också det övergripande ansvaret för att inga otillåtna behandlingar av personuppgifter utförs.

3.4 Verksamhetsansvariga

Sektorschefen eller verksamhetschef, genom sina avdelningschefer och tillsammans med verksamhetens eventuella IT-samordnare, är ansvarig för att driva verksamheten. Ur IT-säkerhetssynpunkt betyder detta bland annat att ansvara för själva informationen i sin egen verksamhets system och att denna hanteras på ett från säkerhetssynpunkt tillfredställande sätt.

Inom ramen för nämndens resurstilldelning ansvarar verksamhetsansvarig för att fastställa säkerhetsnivån för datasystemet i en systemsäkerhetsplan. Alla system skall minst uppnå grundsäkerhet.

Detta innebär att fastställa:

- Vilket informationsinnehåll datasystemet skall ha
- Organisation och befattningar som rör systemet
- Vilka lagar och andra regelverk som gäller
- Identifiera verksamhetsrelaterade krav på datasystemet
- Identifiera hotrelaterade krav för datasystemet
- En säkerhetsinstruktion för datasystemet
- En i samverkan med IT-ansvarig avbrottsplan för datasystemet
- Datasystemets dokumentation och användarhandledning
- Driftgodkännanden av nya datasystem
- Utbildningsbehovet av systemet
- Hur systemet fungerar ihop med andra system (i samråd med IT-enheten)
- Beslut om utveckling av datasystemet ifråga om nya funktioner och samverka med IT-enheten då systemförändringar aktualiseras.
- Systemets ekonomi med avseende på utveckling och användning. När det gäller den tekniska driften sker diskussionen med IT-enheten.
- Informationsinnehållet (personuppgiftsansvariga).
- Beslut om enskilda användares behörighet till datasystemet
- Hur och av vem/vilka informationen skall registreras i systemet.
- När personal slutar eller av annat skäl skall ha ändrade behörigheter samt meddela detta till IT-enheten.

Inom Verksamhetsansvarigs område ligger också att svara för att behövliga licenser respektive tillstånd finns för datasystemet.

3.5 Systemförvaltare

Systemförvaltare utses av verksamhetsansvarig och är den person i berörd verksamhet som har ansvaret för den dagliga användningen av datasystemet. Systemförvaltare samverkar med IT-enheten för att säkerställa en säker och rationell drift av systemet.

Systemförvaltare har som uppgift att:

- Verkställa beslut som systemägaren och verksamhetsansvarig fattar.
- Dokumentera förslag till ändringar/utveckling av systemet
- Ge användarsupport beträffande verksamhetsrelaterade frågor i systemet
- Samverka med IT-enheten
- Genomföra erforderliga utbildningar i systemet
- Svara för användar- och behörighetsadministration
- Delta i arbetet med säkerhetsfrågor som rör systemet

3.6 IT-enheten

IT-enheten ansvarar för Höör kommuns IT-infrastruktur och har det övergripande ansvaret för att infrastrukturen fungerar tillsammans med de olika verksamhetssystemen. IT-enheten samverkar med systemägare och verksamhetsansvariga med avseende på drift och resursfördelning för ett datasystem

IT-enheten har följande ansvarsområden:

- Tillsammans med IT-säkerhetsfunktionen årligen se över IT-säkerhetspolicyn
- Att driftsmiljön för ett datasystem håller den tekniska och funktionella kvalitet som överenskommits med verksamhetsansvarig.
- Att i samråd med verksamhetsansvarig, se till att systemet fungerar ihop med samverkande datasystem
- Att rutiner för säkerhetskopiering finns.
- Att säkerhetskopierat material förvaras på ett betryggande sätt och kontrollera att återläsningsrutiner fungerar.
- Att reservrutiner finns så att verksamhetsansvarigs krav på längsta tillåtna avbrottstid kan tillgodoses.
- Att biträda verksamhetsansvarig i avbrottsplaneringen.
- Att vara teknisk rådgivare till verksamhetsansvarig då förändringar i systemet är aktuella.
- Att nätverk och kommunikation har tillräcklig kapacitet.
- Att ansvara för systemets tekniska säkerhet
- Anpassa IT-säkerheten till den nivå som ställs av de system som kräver störst säkerhet
- Registrera användare i nätet (infrastrukturen) men den behörighetsprofil som verksamhetsansvarig har beslutat.
- Avregistrera användare (infrastrukturen) efter verksamhetsansvarigs beslut.
- Ansvara för, tillsammans med systemansvarig, att den dagliga driften upprätthålls enligt överenskommelse mellan operativa verksamheten och IT-enheten.
- Vara rådgivande till systemägarna och verksamhetsansvariga i IT-säkerhetsfrågor.
- Biträda verksamhetsansvariga vid upprätthållande av;
    - Säkerhetsinstruktioner
    - Avbrottsplanering för verksamheten
    - Säkerhetsgranskning inför driftsgodkännande
- Biträda vid utbildning i IT-säkerhetsfrågor samt
- Samordna rapportering av incidenter för vidare uppföljning med systemägare och kommunens säkerhetsansvarige.

3.7 Användare

Varje användare är skyldig att följa regler och anvisningar som anges i IT-säkerhetspolicyn och IT-säkerhetsinstruktioner. I detta ansvar ingår även att noga ta del av och följa de säkerhetsinstruktioner som finns för de enskilda datasystem den användaren utnyttjar.

3.8 IT-säkerhetsfunktion

Räddningstjänsten i Höörs kommun har ansvaret för att samordna säkerheten. I IT-säkerhetsarbetet innebär det att understödja arbetet med att uppnå IT-säkerhetspolicyns mål. Detta kan innebära aktivt deltagande i projekt, etablerande av interna och externa kontaktnät, utvärdering och deltagande i diskussioner kring metoder, plattformar, applikationer eller datasystem Ansvaret innebär också att tillsammans med IT-chef årligen se över IT-säkerhetspolicyn. Denna uppgift måste ligga utanför IT-enheten som annars kommer att granska sig själv.

4 Lagar och andra regelverk

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

Detta omfattar bland annat:

- Skyddet av den personliga integriteten reglerad genom personuppgiftslagen.
- 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 samt.
- Speciallagstiftning, ex. socialtjänstlagen, hälso- o sjukvårdslagen.
- Att upphovsrättsskyddat material inte felaktigt sprids eller lagras på kommunens datorer

5 IT-säkerhetsarbetet inom Höör kommun

IT-säkerhetsarbetet inom Höör kommun skall följa den process som baseras på Krisberedskapsmyndighetens (KBM:s) skrivelse 2003:2 (BITS)

- Utgående från säkerhetsplanen tas en systemsäkerhetsplan fram för varje enskilt datasystem. I systemsäkerhetsplanen identifieras, utöver den lägsta säkerhetsnivån som gäller för Höör kommun, även krav i lagar och andra regelverk, verksamhetsrelaterade krav och hotrelaterade krav. Systemsäkerhetsplanen fastställs av verksamhetsansvarig.
- Utgående från IT-säkerhetspolicyn och systemsäkerhetsplanen skall säkerheten diskuteras för varje enskilt verksamhetssystem och om så anses nödvändigt skall kompletterande säkerhetsinstruktioner tas fram.
- För varje verksamhetssystem skall en avbrottsrutin diskuteras och ev. avbrottsplan upprättas.
- Nödvändiga säkerhetsåtgärder vidtas för att tillgodose uppsatta krav på säkerhet.
- Verksamhetsansvariga driftgodkänner nya datasystemet.

IT-chefen rapporterar kring IT-säkerhetsarbetet vid två tillfällen per år till KS AU och KS.

6 Driftgodkännande

Verksamhetsansvariga skall besluta om driftsgodkännande av varje enskilt nytt datasystem. Av beslutet skall framgå hur kraven på grundsäkerhet är tillgodosedda samt hur säkerhet i övrigt tillgodoses. Beslut om driftgodkännande skall dokumenteras.

Alla nya system inom Höör kommun skall ha en sådan säkerhet att de kan driftgodkännas. Säkerhetsarbetet skall för varje nytt system bedrivas så att driftgodkännande kan beslutas innan driftsstart. De åtgärder som då eventuellt återstår skall vara dokumenterade och det skall finnas en tidplan för när de skall vara genomförda.

BILAGA 1 STYRANDE DOKUMENT – ÖVERSIKT

Dokument	Nivå	Innehåll	Upprättas av	Fastställs av
IT-säkerhetspolicy	Generell	Mål för IT-säkerheten vid Höör kommun	IT-chef	KF
IT-säkerhetsinstruktion	Generell	Beskrivning av hur säkerhetspolicyn realiseras.	IT-chef	KS
Systemsäkerhetsplan	Per system	Säkerhetsplan per system	Verksamhetsansvarig	Sektorschef
IT-strategi	Generell	Beskrivning av IT:s syfte och mål i Höör kommun	IT-chef	KS
e-post och internetregler	Generell	Regler för användning av e-post och Internet i Höörs Kommun	IT-chef	KS