

IT-SÄKERHETSPLAN - FALKÖPINGS KOMMUN

1	INLEDNING.....	1
2	MÅL FÖR IT-SÄKERHETSARBETET	1
3	RIKTLINJER FÖR ATT UPPNÅ MÅLEN	1
3.1	ALLMÄNT	1
3.2	LEDNING OCH ANSVAR FÖR IT-SÄKERHET	2
3.2.1	<i>Systemägare</i>	2
3.2.2	<i>Systemansvarig</i>	3
3.2.3	<i>IT-chef</i>	4
3.2.4	<i>Systemtekniskt ansvarig</i>	4
3.2.5	<i>Användare</i>	5
3.2.6	<i>IT-säkerhetsfunktion</i>	5
4	LAGAR OCH ANDRA REGELVERK.....	5
5	GRUNDSÄKERHET IT.....	5
6	IT-SÄKERHETSARBETET INOM FALKÖPINGS KOMMUN.....	5
	BILAGA 1 ÖVERSIKT - STYRANDE DOKUMENT.....	7

1 INLEDNING

Denna säkerhetsplan anger Falköpings kommuns mål för IT-säkerheten samt riktlinjer för hur dessa skall uppnås. Säkerhetsplanen avser kommunens samtliga nätverk och datorer. I dessa finns fler än 100 olika datasystem. Ett stort antal av dem kan klassas som verksamhetskritiska. IT-säkerhetsplanens mål konkretiseras i en generell systemsäkerhetsplan. I de fall systemägaren bedömer att ett verksamhetskritiskt system kräver en högre säkerhetsnivå än den generella, skall det finnas en särskild systemsäkerhetsplan för det enskilda datasystemet. Det åligger systemägaren att ta fram eventuella kompletterande systemsäkerhetsplaner och därtill hörande säkerhetsinstruktioner. En översikt över samtliga styrande dokument och vem som fastställer dessa, återfinns i **bilaga 1**.

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

IT-säkerhetsplanen har upprättats som ett led i kommunens IT-säkerhetsarbete. Säkerhetsarbetet och planerna följer i många fall Kris och Beredskaps Myndighetens (KBM) rekommendationer, Basnivå för IT-säkerhet (BITS). Planerna omfattade ursprungligen enbart det administrativa nätverket. Under 2004 reviderades och omarbetades dessa så att de nu omfattar kommunens samtliga nätverk.

2 MÅL FÖR IT-SÄKERHETSARBETET

Målen för Falköpings kommuns IT-säkerhetsarbete är att:

- samtliga verksamhetskritiska datasystem inom Falköpings kommun minst skall uppnå kommunens grundsäkerhetskrav (baserade på BITS),
- för de datasystem där så anses nödvändigt skall, utöver grundsäkerheten, verksamhetsrelaterade och hotrelaterade krav fastställas i särskild systemsäkerhetsplan,
- säkerhetsinstruktioner och åtgärder i datasystemen utformas och förvaltas på ett sådant sätt att kraven uppfylls,
- en återkommande uppföljning och kontroll av IT-säkerheten skall ske, bl.a. som underlag för verksamhetsplanering samt att
- Falköpings kommun skall kunna utföra sina uppgifter på ett tillfredsställande sätt i samband med svåra påfrestningar.

3 RIKTLINJER FÖR ATT UPPNÅ MÅLEN

3.1 Allmänt

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

- gällande lagar, föreskrifter och författningar följs,
- alla användare har kunskap om Falköpings kommuns IT-säkerhetsregler,
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för datakommunikation,
- informationen skall vara tillgänglig för de som har behov av den i sitt arbete men inte för någon annan samt
- löpande analysera hotbilden för varje enskilt verksamhetskritiskt datasystem

3.2 Ledning och ansvar för IT-säkerhet

En fastställd ansvarsfördelning för IT-säkerheten är en avgörande förutsättning för Falköpings kommun att leva upp till sin IT-säkerhetsplan. 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 en fördjupad beskrivning av ansvarsfördelningen för olika rollinnehavare. I vissa fall kan samma person inneha fler än en av dessa roller.

3.2.1 Systemägare

I Falköpings kommun är den som är verksamhetsansvarig också systemägare. Detta innebär för de förvaltningsövergripande verksamhetssystemen (t.ex. ekonomisystem och ärendehanteringssystem) att kommunstyrelsen är systemägare och kommundirektören den som utövar systemägaransvaret. För de generella resurserna i nätverken (t.ex. nätverksoperativ, antivirusprogram, e-post och kontorsprogram mm) utövar IT-chefen systemägaransvaret. Vad gäller de förvaltnings specifika systemen är respektive nämnd systemägare och förvaltningschefen utövar systemägaransvaret. I de fall flera förvaltningar delar ett system skall en av dessa tilldelas systemägaransvaret. Systemägaren har det övergripande ansvaret för att datasystemet förvaltas på för verksamheten bästa sätt. Systemägaren fattar också de avgörande besluten om inköp, vidareutveckling eller avveckling av datasystemet inom ramen för resurstilldelningen för sin verksamhet.

Systemägaransvaret innebär att kommundirektör, IT-chefen och förvaltningschefer har, inom ramen för respektive styrelse och nämnds resurstilldelning, bl.a. ansvar för följande:

- att fastställa säkerhetsnivån för de egna datasystemen. I de fall säkerhetsnivån i den generella systemsäkerhetsplanen inte bedöms som tillräcklig skall en särskild systemsäkerhetsplan upprättas för det egna datasystemet.

Detta innebär att fastställa:

- vilket informationsinnehåll datasystemet skall ha
- vilka lagar och andra regelverk som gäller
- identifiera verksamhetens krav på datasystemet
- hotbilden för datasystemet
- att fastställa särskilda säkerhetsinstruktioner för datasystemet.

Systemägaransvaret innebär dessutom att:

- fastställa organisation och befattningar som rör systemet.
- utse systemansvarig.
- vid behov, fastställa avbrottsplan och reservrutiner för datasystemet.
- fastställa datasystemets dokumentation och användarhandledning.
- tillse att det finns serviceavtal m.m.
- besluta om utbildning som rör systemet.
- följa upp och utvärdera effekterna av gjorda IT-investeringar.
- bevaka utvecklingen inom det egna verksamhetsområdet och initiera nya IT-lösningar.

- i samråd med IT-chefen, ansvara för att systemet fungerar ihop med samverkande datasystem.
- fatta beslut om systemets ekonomi vad avser utveckling och användning av datasystemet ifråga samt samverka med IT-chefen vad avser teknisk drift och då systemförändringar aktualiseras.

Inom systemägarens område ligger också att ansvara för att behövliga licenser och tillstånd finns för datasystemet. Licensinnehavet skall vara dokumenterat och kontrolleras regelbundet.

3.2.1.1 Informationsansvar

Kommundirektören, IT-chef och förvaltningscheferna ansvarar genom sitt verksamhetsansvar även för själva informationen i systemen och att denna hanteras på ett ur säkerhetssynpunkt tillfredställande sätt.

Informationsansvaret innebär ansvar för:

- vilka uppgifter som skall tillhandahållas enligt offentlighetsprincipen och hur detta skall ske.
- om och vilka delar av informationen som är sekretessbelagd.
- informationsinnehållet (registeransvarig).
- personuppgifter (personuppgiftsansvar).
- beslut om enskilda användares behörighet till det egna datasystemet.
- hur och av vem/vilka informationen skall registreras i systemet
- hur informationen skall arkiveras när system avvecklas samt
- att anmäla till systemansvarig och till IT-avdelningens behörighetsadministration när en användare börjar och slutar sin anställning eller skall ha ändrade behörigheter.

3.2.2 Systemansvarig

Systemansvarig utses av systemägaren och är den person i berörd verksamhet som har ansvaret för den dagliga användningen av datasystemet. Systemansvarig samverkar med IT-avdelningens systemtekniker för att säkerställa en säker och rationell daglig drift av systemet.

Systemansvarig har som uppgift att:

- ha det operativa ansvaret för IT-säkerheten i det egna systemet.
- verkställa de beslut som systemägaren fattar.
- dokumentera förslag till ändringar/utveckling av systemet.
- ge användarsupport beträffande verksamhetsrelaterade frågor i systemet.
- genomföra erforderliga utbildningar i systemet.
- vara kontaktperson gentemot leverantörens kundtjänst och supportavdelning.
- i de system som har en intern loggning av aktiviteter, regelbundet granska dessa och rapportera avvikelser till systemägaren samt vid behov rådgöra med den systemtekniskt ansvarige.
- om inte annat är överenskommet med IT-avdelningens systemtekniker, svara för all användar- och behörighetsadministration i det egna datasystemet.
- att tillsammans med den systemtekniskt ansvarige ansvara för att den dagliga driften upprätthålls enligt den beslutade ansvarsfördelning.
- i god tid innan beslut tas om uppdateringar eller förändringar i systemet rådgöra med den

systemtekniskt ansvarige om att förändringarna är tekniskt möjliga att genomföra.

- tillsammans med den systemteknisktansvarige planera lämplig tidpunkt för installationer och uppgraderingar mm.
- delta i arbetet med säkerhetsfrågor som rör systemet.

3.2.3 IT-chef

IT-chefen är ansvarig för Falköpings kommuns IT-infrastruktur och har det övergripande ansvaret för att de olika datasystemens tekniska delar fungerar. IT-chefen utövar också systemägaransvaret för kommunens generella datasystem. Dessutom skall IT-chefen samverka med systemägarna vad avser drift och resursfördelning för datasystemen.

IT-chefen har följande ansvarsområden:

- att i samråd med systemägaren tillse att systemet fungerar ihop med samverkande datasystem,
- att besluta om behörighet till de gemensamma resurserna och infrastrukturen,
- att besluta om avregistrering av användare från de gemensamma resurserna och infrastrukturen,
- att rutinerna för säkerhetskopiering uppfyller systemägarens krav,
- att säkerhetskopierat material förvaras på ett betryggande sätt och kontrollera att återläsningsrutiner fungerar,
- att tillhandahålla teknisk support till användarna, (IT-support),
- att vara teknisk rådgivare till systemägaren då förändringar i systemet är aktuella,
- att ansvara för att det finns en aktuell förteckning över kommunens IT-system.
- att ansvara för att den tekniska IT-säkerheten ligger på en nivå som motsvarar de ställda kraven.

3.2.4 Systemtekniskt ansvarig

Den systemtekniskt ansvarige tillhör IT-avdelningen och innehar den tekniska kompetensen. Systemtekniker, tillsammans med systemansvarig, ansvarar för att den dagliga driften upprätthålls enligt gällande ansvarsfördelning mellan systemägaren och IT-chefen.

Den Systemtekniskt ansvarige har som uppgift att:

- registrera användare och ge dem tillgång till de system som *systemägaren* har beslutat och med den behörighetsprofil som krävs för att utföra sina arbetsuppgifter. Behörighetsprofilen beslutas av IT-chef och administreras av särskilt utsedda systemtekniker.
- avregistrera användare efter anmälan från *systemägaren* och beslut av IT-chefen. Detta administreras av särskilt utsedda systemtekniker.
- tillsammans med systemansvarig ansvara för att den dagliga driften upprätthålls enligt den beslutade ansvarsfördelning.
- ansvara för att systemet rent tekniskt fungerar väl ur tillgänglighetssynpunkt.
- tillhandahålla teknisk support till systemansvarig och användare.
- själva eller tillsammans med leverantörens tekniker ansvara för installation och uppdatering av systemen.
- vara kontaktperson gentemot leverantörens tekniker.

- ansvara för den tekniska dokumentationen kring systemet.
- ansvara för den tekniska säkerheten i systemet och delta i arbetet med säkerhetsfrågor som rör den tekniska infrastrukturen.

3.2.5 Användare

Varje användare är skyldig att ta del av och följa gällande säkerhetsinstruktioner för de datasystem som denne nyttjar. Användaren har också ansvar för att rapportera olika former av incidenter till systemansvarig.

3.2.6 IT-säkerhetsfunktion

Den som innehar en IT-säkerhetsfunktion skall understödja arbetet med att uppnå säkerhetsplanens mål. Detta kan innebära aktivt deltagande i projekt, etablerande av interna och externa kontaktnät, utvärdering och deltagande i diskussioner kring metoder, tekniska plattformar, applikationer eller datasystem.

Det är dock alltid upp till verksamheterna att välja på vilket sätt och med vilka resurser man vill uppnå målen.

4 LAGAR OCH ANDRA REGELVERK

Ramarna för Falköpings 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 av 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 samt
- speciallagstiftning

5 GRUNDSÄKERHET IT

Till grund för Falköpings kommuns IT-säkerhet gäller Basnivå för IT-säkerhet, BITS. Dessa rekommendationer har tillrättalagts utifrån Falköpings kommuns behov och gäller som lägsta säkerhetsnivå i Falköpings kommuns nätverk.

6 IT-SÄKERHETSARBETET INOM FALKÖPINGS KOMMUN

IT-säkerhetsarbetet inom Falköpings kommun skall i huvudsak följa den process i säkerhetsarbetet som baseras på BITS.

Processen är uppbyggt så att det indirekt anger en logisk arbetsprocess för IT-säkerhetsarbetet.

Detta innebär att:

- Utgående från säkerhetsplanen tas en generell systemsäkerhetsplan fram för kommunens nätverk. Därefter kompletteras denna, där så anses nödvändigt, med en särskild systemsäkerhetsplan för

enskilda verksamhetskritiska datasystem. I dessa systemsäkerhetsplaner identifieras, utöver den grundläggande säkerhetsnivån som gäller generellt för Falköpings kommuns nätverk, även de verksamhetsspecifika kraven i lagar och andra regelverk samt verksamhetsrelaterade krav och hotrelaterade krav som gäller för de enskilda datasystemen.

- Särskilda systemsäkerhetsplaner fastställs av respektive systemägare.
- Med utgångspunkt från IT-säkerhetsplanen och systemsäkerhetsplanerna tas säkerhetsinstruktioner fram. I säkerhetsinstruktionerna fastställer systemägaren vilka säkerhetsregler som gäller för det egna datasystemet.
- De säkerhetsregler som direkt berör användarna beskrivs i ett särskilt dokument.
- För varje verksamhetskritiskt datasystem skall systemägaren bedöma om det finns ett behov av en avbrottsplan. I så fall skall en sådan upprättas.
- För det administrativa nätverket skall det finnas en katastrofplan som beskriver hur en alternativ IT-drift skall initieras, bedrivs och avslutas.
- Nödvändiga instruktioner och säkerhetsåtgärder skall vidtas för att tillgodose kraven i systemsäkerhetsplanen.

BILAGA 1 ÖVERSIKT - STYRANDE DOKUMENT

Dokument	Nivå	Innehåll	Upprättas av	Fastställs av
Säkerhetsplan	Omfattar kommunens båda nätverk	Ansvarsfördelning och övergripande mål för IT-säkerheten i Falköpings kommuns nätverk	IT-chef	Kommunstyrelsen
Generell system-säkerhetsplan	Omfattar kommunens båda nätverk	Konkreta mål och ramar för IT-säkerheten kring kommunens nätverk	IT-chef	Kommundirektör
Särskild system-säkerhetsplan	Per system	Konkreta mål och ramar för IT-säkerheten kring enskilda system	Systemägare	Systemägare
Generell säkerhetsinstruktion	Omfattar kommunens båda nätverk	Generella säkerhetsregler och instruktioner kommunens nätverk	IT-chef	IT-chef
Kompletterande säkerhetsinstruktion	Per system	Särskilda säkerhetsregler för enskilda system	Systemägare	Systemägare
Säkerhetsinstruktion för användare	För alla användare	Generella säkerhetsregler och instruktioner för användare kommunens nätverk	IT-chef	IT-chef
Kompletterande säkerhetsinstruktion	För en grupp av användare	Särskilda säkerhetsregler för användare av enskilda system	Systemägare	Systemägare
Avbrottsplan	Per system	Plan för avbrott	Systemägare	Systemägare
Katastrofplan	Det administrativa nätverket	Plan för katastrof	IT-chef	IT-chef