Dnr
62/2004/100

Gäller fr. o. m.
2004-04-01

Antagen
Kf 2004-03-29 § 22

SÄKERHETSPOLICY – IT

SÄKERHETSPOLICY IT

Innehåll: Sid

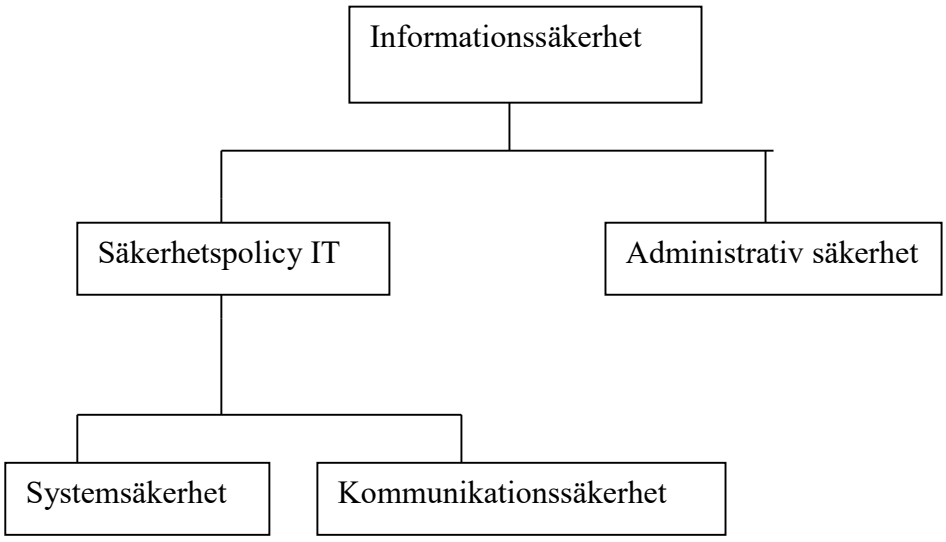
Säkerhetspolicy IT kompletteras av bilaga: Säkerhetsinstruktion IT, för användare

Förord

Krisberedskapsmyndigheten (KBM) har ett sammanhållande myndighetsansvar inom informationssäkerhetsområdet och har kraven på samhällets förmåga att fungera även under olika krissituationer som utgångspunkt. IT-system som betraktas som samhällsviktiga intar en central roll när det gäller olika samhällsfunktioners möjligheter att bedriva sin verksamhet.

Säkerhetspolicy IT är ett projekt för att skapa en gemensam IT-plattform för Karlshamns, Olofströms och Sölvesborgs kommuner, i fortsättningen kallade Blekinge Väst. Våra kommuner har som mål att upprätthålla en fortsatt god Informationssäkerhet. Som ett led i detta har kommunerna beslutat följa KBM´s rekommendationer för IT-säkerhet (BITS). BITS baseras på vedertagna standarder och är till sitt innehåll konsistent med ISO/IEC 17799 avseende IT-säkerhet. Vidare definieras en balanserad basnivå för säkerheten i IT-system.

Säkerhetspolicy IT är underordnad respektive kommuns IT-strategi och skall betraktas som ett förtydligande av det regelverk, som skall gälla för en säker IT-verksamhet.



1. INLEDNING

Det moderna samhället är starkt beroende av att elförsörjning, telekommunikationer och datasystem fungerar. Angrepp mot dessa datasystem kan åstadkomma svåra störningar i samhället. De inbördes beroenden som finns mellan dessa system måste uppmärksammas liksom den tekniska utvecklingen inom dessa områden.

Mycket av den infrastrukturella sårbarheten är kopplad till det stora IT-beroendet som generellt gäller samhällsviktiga funktioner. Störningar i datasystem kan få betydande följdverkningar och svåra konsekvenser för samhället, varför säkerhetsfrågorna inom IT-område spelar en allt mer central roll.

Som grund för Blekinge Väst IT-säkerhet gäller KBM´s rekommendationer ”Basnivå för IT-säkerhet” (BITS).

En god och verksamhetsanpassad IT-säkerhet skall finnas i samtliga tekniska miljöer där informationshantering äger rum.

IT-säkerhetsarbetet i Blekinge Väst skall:

- Garantera hög kvalitet, effektivitet och tillförlitlighet i IT-stödet.
- Hindra och/eller minska effekterna av oönskade händelser.
- Höja säkerhetsmedvetandet hos de anställda
- Skydda medborgarnas integritet samt bidra till att nyttjande av informationsteknik har deras förtroende.

Säkerhetspolicy IT för Blekinge Väst

Säkerhetspolicy IT anger kommunernas mål för IT-säkerheten samt hur denna skall uppnås.

Säkerhetspolicy IT vill understryka att IT-säkerhetsarbetet är ett medel för kommunerna
att försäkra sig om att redan gjorda och kommande investeringar ger förväntad effekt i verksamheterna. Vid framtagandet av Säkerhetspolicy IT har följande beaktats:

- Informationsbehandling med IT-stöd är omfattande och har strategisk betydelse för kommunernas verksamhet.
- Kommunernas medborgare och IT-användare samt samhället i övrigt ställer krav beträffande integritetsskydd och tillförlitlighet i de system som används.
- Lagar och förordningar påverkar användandet av IT-stöd och medför krav på åtgärder.

Hjälpmedel för införande av Säkerhetspolicy IT

Hjälpmedel för säkerhetsarbetet i form av mallar, checklistor mm kommer att finnas att tillgå på respektive kommuns intranät.

2. MÅL FÖR IT-SÄKERHETSARBETET

Målen för kommunernas IT-säkerhetsarbete är att:

- redovisa ledningens viljeinriktning och stöd för IT-säkerhet,
- stödja kommunernas samlade utvecklings- och förbättringsarbete,
- ansvaret, och därmed befogenheter att fatta beslut, skall följa respektive kommuns delegationsordning,
- samtliga datasystem i kommunerna, oavsett om dessa är samhällsviktiga eller inte, skall uppfylla KBM´s basnivå,
- för varje datasystem skall utöver basnivå, verksamhetens tilläggskrav och hotbild definieras och fastställas i en systemsäkerhetsplan,
- säkerhetsåtgärder i datasystemen utformas och förvaltas på ett sådant sätt att verksamhetens krav uppfylls,
- en regelbunden uppföljning och kontroll av IT-säkerheten skall ske, bl. a som underlag för verksamhetsplanering,
- varje datasystem ska formellt driftgodkännas,
- kommunerna skall kunna utföra sina uppgifter på ett tillfredsställande sätt även vid särskilda händelser och under höjd beredskap.

3. RIKTLINJER FÖR ATT NÅ MÅLEN

För att uppnå målen krävs en effektiv samverkan mellan människor, applikationer och teknik vilket förutsätter att:

- gällande lagar, föreskrifter och författningar följs,
- all personal får kunskap om kommunens IT-säkerhetsregler,
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur,
- hotbilden löpande analyseras för varje enskilt datasystem för att identifiera tänkbara angripare.

3.1 Ansvarsfördelning

Kommunstyrelsen har det övergripande ansvaret för respektive kommuns IT-säkerhet. Kommunstyrelsen svarar för kontinuerlig revidering samt uppföljning av hur Säkerhetspolicy-IT efterlevs. Detta sker bland annat genom IT-säkerhetsrådets rapportering till kommunstyrelsen/nämnder.

Ansvarsfördelningen skall säkerställa att ett datasystem uppfyller målen för Säkerhetspolicy-IT. IT-säkerhetsfrågorna skall vara integrerade i verksamheten.

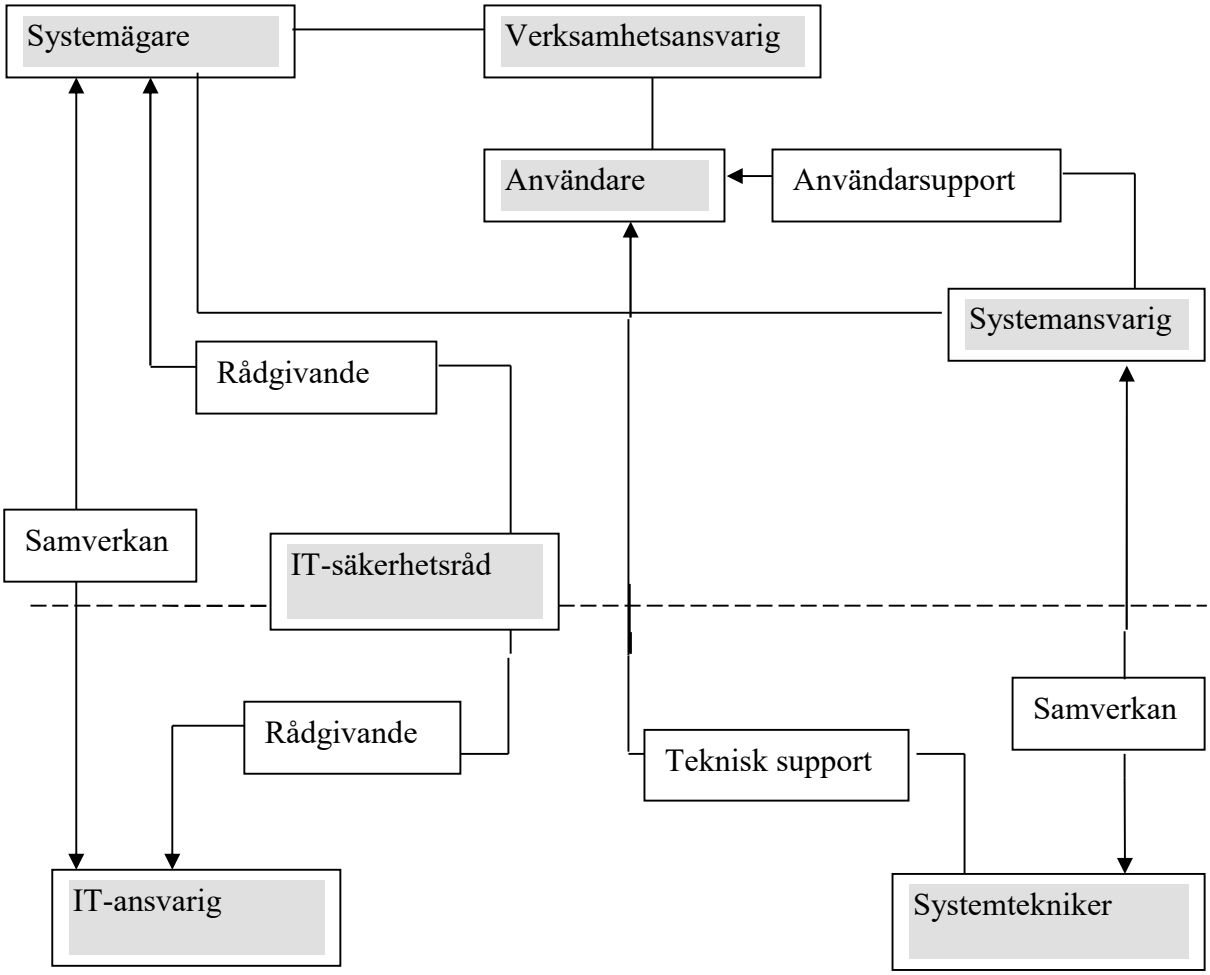
Varje **nämnd och styrelse** är ytterst ansvarig för IT-säkerheten inom sitt område och för att kommunens riktlinjer för informationssäkerhetsarbetet efterlevs.

Nämnd och styrelse svarar för att behandling av personuppgifter sker i enlighet med personuppgiftslagens (PuL) bestämmelser.

Grunden för säkerhetsarbetet inom IT-området är en genomtänkt organisation och riskmedvetna användare. Generellt gäller att var och en som är ansvarig för en verksamhet, också ansvarar för IT-säkerheten inom sitt område.

En viktig del i säkerhetsarbetet är att definiera hur ansvaret för alla IT-system inom kommunen är fördelat på systemägare och övriga roller.

Nedanstående bild och efterföljande text beskriver de olika roller och ansvar för IT-säkerhetsarbetet som finns inom Blekinge Väst.


Systemägare
Verksamhetsansvarig
Användare
Användarsupport
Systemansvarig
Rådgivande
Samverkan
IT-säkerhetsråd
Samverkan
Rådgivande
Teknisk support
IT-ansvarig
Systemtekniker

3.1.1 Systemägare

Systemägare är den **myndighet** (nämnd) i kommunen inom vars verksamhetsområde ett IT-system används, förvaltas och administreras. Kommunstyrelsen (eller annan nämnd) kan vara **central systemägare** till ett system som är gemensamt för hela kommunen och därför används av flera nämnder. Den enskilda facknämnden är då endast användare av IT-systemet och har inget eget förvaltningsansvar för systemet.

Systemägaren har det övergripande ansvaret för att datasystemet förvaltas på bästa sätt för verksamheten. Systemägaren fattar de avgörande besluten om datasystemets anskaffning, utveckling eller avveckling.

3.1.2 Verksamhetsansvariga

Det operativa ansvaret för att datasystemen uppfyller verksamhetens krav vilar på verksamhetsansvariga, till exempel förvaltningschef/funktionsansvarig. I detta ansvar ingår att bedöma den egna verksamhetens krav på säkerhet avseende sekretess, tillförlitlighet, tillgänglighet, spårbarhet samt att personalen har tillräckliga kunskaper för att hantera datasystemet på ett säkert sätt.

3.1.3 Systemansvarig

Systemansvarig är en tjänsteman som genom **delegation** från systemägaren fått i uppdrag att bereda systemärenden för förvaltningsledningen samt att svara för administration, förvaltning och användning av ett IT-system i verksamheten. Systemansvarigs ansvar och arbetsuppgifter bör beskrivas i befattningsbeskrivning. Om delegation inte skett till enskild tjänsteman är myndigheten ansvarig för systemförvaltningen.

3.1.4 IT-ansvarig (IT-chef)

IT-ansvarig är systemansvarig för kommunens tekniska grundstruktur för IT (nätverk, kommunikation mm) och samverkar med systemägare avseende ett datasystems tekniska drift.

3.1.5 Systemtekniker

Systemtekniker innehar den tekniska kompetensen och ansvarar för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och IT-ansvarig.

3.1.6 Användare

Varje användare ansvarar för att gällande regler och riktlinjer för IT-säkerhet följs. I detta ingår att noga ta del av och följa de säkerhetsregler som finns för de datasystem den enskilde användaren använder.

3.1.7 IT-säkerhetsråd

IT-säkerhetsrådet är i säkerhetsfrågor direkt underställt kommunstyrelsen. IT-säkerhetsrådet stödjer kommunens förvaltningar i arbetet med att uppnå målen för Säkerhetspolicy IT.

3.1.8 Regionalt IT-säkerhetsråd

För att följa upp den regionala tillämpningen av Säkerhetspolicy IT skall i Blekinge Väst finnas ett IT-säkerhetsråd med representanter för berörda kommuner. Det regionala IT-säkerhetsrådet skall svara för att samordna revideringen av Säkerhetspolicy IT.

3.2 Lagstiftning och andra regelverk

Ramarna för kommunernas IT-säkerhetsarbete sätts utifrån gällande lagar och förordningar. Dessa anger bland annat de övergripande säkerhetskrav som ställs på verksamheten och därmed även på hanteringen av information i datasystem, vilket bl.a. reglerar:

- skyddet av den personliga integriteten,
- att sekretessbelagd information skyddas mot otillbörlig åtkomst, med iakttagande av offentlighetsprincipen,
- olika intressenters krav på korrekt information och allmänhetens lagliga rätt till insyn i offentliga handlingar.

3.3 Basnivå IT

Som grund för kommunernas IT-säkerhet gäller KBM´s (Krisberedskapsmyndigheten) rekommendationer för IT-säkerhet.

3.4 IT-säkerhetsarbetet inom Blekinge Väst

För varje datasystem inom Blekinge Väst skall en Systemsäkerhetsplan utarbetas med utgångspunkt från Säkerhetspolicy IT. I Systemsäkerhetsplanen identifieras, utöver Basnivå för IT-säkerheten, styrande lagkrav, verksamhetskrav för sekretesskydd, tillförlitlighet, tillgänglighet, spårbarhet samt hotbild. Systemsäkerhetsplanen skall fastställas av systemägaren.

3.5 Driftgodkännande

Systemägaren skall för vart och ett av sina datasystem besluta om driftgodkännande Av beslutet skall framgå hur kraven på bassäkerhet och eventuella specifika tilläggskrav från verksamheten tillgodoses av Systemsäkerhetsplan. Beslut om driftgodkännande skall dokumenteras.

———