Informationssäkerhetspolicy för Vetlanda kommun

Dokumenttyp:	Policy
Beslutad av:	Kommunfullmäktige (2015-12-16 § 202)
Gäller för:	Alla kommunens verksamheter
Giltig fr.o.m.:	2015-12-16
Dokumentansvarig:	IT-strateg/processutvecklare (kommunkansliet)
Senast reviderad:	2015-12-16 (kommunfullmäktige § 202)
Senast granskad:	2015-12-16

Innehållsförteckning

Informationssäkerhetspolicy för Vetlanda kommun 1

Inledning 3

Begreppsförklaring 3

Syfte 4

Mål för Informationssäkerhetsarbetet 5

Långsiktiga mål 5

Årliga mål 5

Organisation, roller och ansvar 6

Övergripande ansvar 6

Kommunstyrelse 6

Nämnd 6

Ledning och ansvar för informationssäkerhet 6

Verksamhetsansvarig (systemägare) 6

Systemansvarig 7

IT-strateg 7

Höglandets kommunalförbund 8

Särskilda områden 9

Systemförvaltning 9

Systemanvändning 9

Kontinuitetsplanering 9

Driftgodkännande 9

Revidering och uppföljning 10

Inledning

Sedan den 1 januari 2010 finns en för Höglandskommunerna gemensam samverkansplattform för drift och underhåll av IT-verksamheten. IT-verksamheten finns inom Höglandets Kommunalförbund (HKF) och är en del av direktionens ansvar. Beslutanderätten avseende IT-verksamhetens mål, inriktning, omfattning och kvalitet ligger inom HKF. Till sin hjälp att utöva sitt ansvar inom HKF finns kommunchefsgruppen som en resurs. De e-strategiska utvecklingsfrågorna är ett ansvar för de kommunala verksamheterna.

Verksamhetsansvar innebär ansvar för verksamhetssystem och därmed informationssäkerheten. Verksamhetsansvarig är systemägare och ska upprätta systemsäkerhetsanalyser för verksamhetskritiska system. Detta kräver en part inom Höglandets IT för att stödja och kvalitetssäkra verksamheternas informationssäkerhet. Överenskommelser kring informationssäkerhet tecknas mellan verksamhetsansvariga/systemägare och Höglandet IT.

Information är en värdefull tillgång, den är kopplad till verksamhetens processer och måste skyddas efter behov. En lång rad lagar och förordningar ska uppfyllas. Förutom arkivlagen finns till exempel den grundlagsstyrda insynsrätten, det vill säga sekretesslagen, tryckfrihetsförordningen med offentlighetsprincipen och personuppgiftslagen. En väl fungerande e-förvaltning kräver en strukturerad hantering av den digitala informationen som ska få genomslag under informationens hela livscykel. Informationssäkerhetarbetet innebär ett systematiskt och långsiktigt arbete som omfattar riktlinjer, rutiner samt tekniskt skydd.

Informationssäkerhet är en del i kommunens lednings- och kvalitetsprocess som ska bidra till att ett informationssystem kan användas på avsett sätt och med avsedd funktionalitet. Informationssäkerhetsarbetet bör följa det av MSB (Myndigheten för Samhällsskydd och Beredskap) rekommenderade ramverk LIS, inom ISO 27000-serien.

(*Standardserien omfattar ledningens ansvar, administrativa rutiner och övergripande krav på IT-infrastruktur. Det finns möjlighet till oberoende certifiering av informationssäkerheten, i likhet med standarder för kvalitet ISO 9000 och miljö ISO 14000*)

Begreppsförklaring

Informationssäkerhet är säkerhet beträffande informationstillgångar rörande förmågan att:

- den alltid finns där när vi behöver den (tillgänglighet)
- vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- endast behöriga personer får ta del av den (konfidentialitet)
- det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet)

Informationstillgångar är en organisations informationsrelaterade tillgångar, det vill säga både information och de resurser som används för att hantera information (exempelvis mjukvaror såsom kunddatabas, program, applikationer, operativsystem, kommunikationstjänster och hårdvaror såsom datorer och nätverk).

LIS, ledningssystem för informationssäkerhet, är ett verktyg för att upprätta, införa, driva, övervaka, granska, underhålla och förbättra den önskade nivån på informationssäkerhet i organisationen.

Med **informationssäkerhetspolicy** menas här den övergripande viljeinriktningen för informationssäkerhet. Den ska ange varför det är viktigt med informationssäkerhet, mål och ansvarsförhållanden och uttrycker inga konkreta förhållningsregler, föreskrifter eller rutinbeskrivningar.

Syfte

Vetlanda kommuns informationstillgångar ska skyddas på ett sätt som tillgodoser legala krav, medborgarintressen och verksamhetsmässiga mål.

Denna informationssäkerhetspolicy är ett styrande dokument som anger en viljeinriktning och ett stöd för informationssäkerhetsarbetet och syftar till att klargöra:

- Långsiktiga och kortsiktiga mål för informationssäkerhetsarbetet
- Organisation, ansvar och roller inom informationssäkerhetsområdet
- Särskilda rutiner för informationssäkerhet

Mål för Informationssäkerhetsarbetet

Långsiktiga mål

De **långsiktiga** målen för informationssäkerhetsarbete är att säkerställa att kommunen, på ett lagligt och säkert sätt, kan tillhandahålla relevant information som:

- Endast delges behöriga personer (konfidentialitet) och kan levereras vid rätt tidpunkt och till skäliga kostnader
- Är riktig, komplett och aktuell (tillförlitlig och riktighet)
- Efterfrågas och som kommunen har ett ansvar att tillhandahålla (tillgänglighet)
- Går att följa hur den har hanterats (spårbarhet)

För att uppnå dessa mål ska kommunens informationssäkerhetsarbete bedrivas så att:

- Lagar och föreskrifter följs
- Det stöder kommunens samlade utvecklingsarbete och säkrar en effektiv informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande parter och tredje man
- Det förebygger oväntade händelser i informationssystemen som kan leda till negativa konsekvenser. Hotbilden för varje enskilt samhällsviktigt och verksamhetskritiskt informationssystem analyseras fortlöpande och det finns systemförvaltningsplaner och säkerhetsinstruktioner upprättade för dessa system
- Alla investeringar både i form av information (data) och teknisk utrustning skyddas i tillräcklig grad. Kommunens information ses som en tillgång och skyddas i paritet med dess värde
- Samtliga system som finns inom kommunen ska vara identifierade och det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- All personal ges kunskap om gällande informationssäkerhetsregler

Årliga mål

Informationssäkerhetsarbetet ska bedrivas som en integrerad del av kommunens normala verksamhet. Årliga mål för arbetet bör beslutas av systemägare.

De årliga målen bör ange:

- Vad som ska göras under året och en tidplan (när och hur, sluttidpunkt)
- Resurser för arbetet (personella och ekonomiska)
- När, hur och av vem som uppföljning, utvärdering och avrapportering ska ske till systemägare
- När och hur kommunens medarbetare ska informeras och utbildas

Organisation, roller och ansvar

Övergripande ansvar

Alla har ett ansvar för att informationssäkerheten upprätthålls och fungerar enligt lagar och regelverk. Det övergripande ansvaret för kommunens informationssäkerhet har kommunfullmäktige och är ägare till detta styrdokument. Säkerhetsansvaret för varje enskilt informationssystem följer verksamhetsansvaret. Den som upptäcker brister i informationssäkerheten måste uppmärksamma till exempel sin chef på detta. Alla medarbetare måste också rapportera händelser som kan göra att informationstillgångar utsätts för risker.

Kommunstyrelse

Kommunstyrelsen (KS) ska leda och samordna den övergripande styrningen av kommunens informationssäkerhet.

Nämnd

De olika nämnderna ska säkerställa att registerhållningen inte strider mot personuppgiftslagen (PUL).
Riktlinjer och rutiner beslutas i enlighet med ”Riktlinjer för kommunens styrdokument”.

Ledning och ansvar för informationssäkerhet

En fastställd ansvarsfördelning för informationssäkerheten är en avgörande förutsättning för att Vetlanda kommun ska kunna leva upp till sina åtaganden. Organisation, roller och fördelning av ansvar ska säkerställa att ett informationssystem kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla informationssäkerhetspolicyns mål. Detta innebär att ett informationssystem med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial med mera.

Verksamhetsansvarig (systemägare)

Verksamhetsansvarig ansvarar för att de system för vilka man är systemägare, hanteras på ett ur säkerhetssynpunkt tillfredsställande sätt. Verksamhetsansvarig kan vara förvaltningschef eller motsvarande. Systemägare ansvarar inför sin nämnd.

Systemägarens grundläggande ansvar för informationssäkerhet innebär att:

- Fastställa vilket informationsinnehåll systemen ska ha samt vilka lagar och andra regelverk som gäller
- Identifiera verksamhetskritiska system, verksamhetskrav och hotbild för systemen
- Fastställa säkerhetsinstruktioner för systemen, bland annat
    - hur och av vem eller vilka informationen ska registreras i systemet
    - vilka uppgifter som ska tillhandahållas enligt offentlighetsprincipen och hur detta ska ske

- I samverkan med leverantör fastställa systemförvaltnings- och avbrottsplan samt driftgodkänna system
- Besluta om enskilda användares behörighet till informationssystemet samt tillse att avregistrering sker när förutsättningarna har ändrats och användaren inte längre ska ha tillgång till systemet.
- Arbeta fram en prioritering mellan informationssystem vid större haverier, dvs. regler för vilka system som ska startas upp respektive stängas ned. Detta görs tillsammans med den eller de som är utsedda att ha ett för kommunen övergripande ansvar för informationssäkerhet samt driftleverantör

Systemansvarig

Systemansvarig utses av systemägare och är den person i berörd verksamhet som har ansvaret för den dagliga administrationen av informationssystemet. Systemansvarig samverkar med Höglandets IT för att säkerställa en säker och rationell daglig drift av systemet.

Systemansvarig har som uppgift att:

- Verkställa beslut som systemägaren/verksamhetsansvarig fattar
- Klargöra och dokumentera e-relaterade behov och förslag inom verksamhetsområdet
- Klargöra verksamhetsområdets krav tillsammans med berörda (kravspecificering)
- Se till att nödvändig dokumentation finns, att rätt säkerhets- och servicenivåer är klargjorda
- Följa upp och utvärdera beställningar och servicenivåer
- Vara kontaktperson och samverka med Höglandets IT
- Svara för användar- och behörighetsadministration
- Delta i arbetet med säkerhetsfrågor som rör systemet

IT-strateg

Uppdraget som IT-strateg är att driva och stödja den kommunala verksamhetens förändring mot den framtida agendan för e-förvaltning. Detta utifrån bland annat medborgarperspektivet, näringslivsperspektivet, nationella initiativ och regional samverkan. Detta inkluderar även aspekterna kring informationssäkerhet.

IT-strategens ansvar för informationssäkerhet innebär att:

- Tillse att verksamhet och den digitala omställningen går hand i hand
- Bereda och skapa beslutsunderlag avseende övergripande och strategiska informationssäkerhetsfrågor
- Ständigt förbättra och kvalitetssäkra det strategiska säkerhetsarbetet
- Stödja verksamheten med att följa upp åtaganden avseende överenskomna servicenivåer (SLA) och leveranser från leverantörer
- Utveckla och etablera ramverk (metoder och rutiner) för informationssäkerhetsarbetet

Höglandets kommunalförbund

Höglandets kommunalförbund ansvarar för IT-säkerhetspolicy för dess verksamhet och anslutna medlemskommuner. Denna är ett komplement till höglandskommunernas policy för informationssäkerhet.

HKF och Höglandets IT understödjer arbetet med att uppnå kommunernas mål för informationssäkerhet. Detta kan innebära aktivt deltagande i projekt, etablerande av kontaktnät, utvärdering och deltagande i diskussioner kring metoder, plattformar, applikationer eller informationssystem. Det är dock alltid upp till verksamheterna att välja på vilket sätt man vill uppnå målen.

Höglandets IT har till uppgift att:

- driften av infrastruktur och system sker på ett säkert sätt
- vara rådgivande till systemägarna i informationssäkerhetsfrågor
- biträda systemägarna vid upprättande av
    - systemförvaltningsplan
    - säkerhetsinstruktioner
    - avbrottsplanering för verksamheten
    - säkerhetsgranskning inför driftgodkännande
- vara rådgivande till systemägare vad avser teknisk säkerhet
- samordna rapportering och uppföljning av incidenter

Särskilda områden

Vissa områden inom informationssäkerhet är av särskild betydelse för kommunens verksamhet och behöver därför särskilda rutiner. Följande områden ska beskrivas i särskilda instruktioner.

Systemförvaltning

Arbetet med systemförvaltning syftar till att följa verksamhetens behov och krav, inte minst informationssäkerheten, och tillgodose dessa. Befintliga funktioner och tjänster ska underhållas och nya implementeras för att klara säkerhets- och kvalitetskrav. Systemförvaltningsplanen beskriver de system planen avser och de beroenden (integrationer) som är nödvändiga för systemets funktion och tillämpning. Detta gäller framför allt verksamhetskritiska system. Verksamhetskritiska system bör därför regelbundet identifieras och klassificeras. Systemförvaltningsplanen är ett ansvar för systemägaren.

Systemanvändning

En del av säkerhetsarbetet avser hur vi ska använda systemen på ett säkert sätt. Det gäller bland annat behörigheter, hantering av information, e-post, distansarbete och användning av internet. Detta är säkerhetsinstruktioner som vänder sig till användare av kommunens system och beslutas av kommunstyrelsen.

Kontinuitetsplanering

Utifrån kommunens och systemägarnas krav på de enskilda informationssystemen, ska avbrotts- och katastrofplaner upprättas och ajourhållas för den tekniska infrastrukturen. För denna kontinuitetsplanering ansvarar driftsorganisationen för informationssystemen.

Driftgodkännande

Systemägaren ska besluta om driftgodkännande av varje enskilt informationssystem i samband med driftagande av förändringar eller av nya system. Av beslutet ska framgå hur kraven på informationssäkerheten tillgodoses. Beslut om driftgodkännande ska dokumenteras.

Revidering och uppföljning

Policy och de särskilda rutinerna för informationssäkerhet ska löpande följas upp och ingå i den interna kontrollen.