Informationssäkerhetspolicy

Antagen av kommunfullmäktige den 2009-10-21, §110

Kommunstyrelseförvaltningen

Postadress	Besöksadress	Telefon	Telefax	E-post	Hemsida
462 85 Vänersborg	Sundsgatan 29	0521-72 10 00	0521-72 19 60	vanersborg.kommun@vanersborg.se	www.vanersborg.se

Innehåll

Informationssäkerhetspolicy

Tillägg

1. Informationssäkerhet

Olika typer av hot och säkerhetsincidenter utgör en risk för Vänersborgs kommuns verksamhet. Förlust, förstörelse eller förändring av data eller oauktoriserat offentliggörande av sekretessbelagd information från våra system kan göra det svårt eller omöjligt för vår personal att utföra sin uppgift eller utsätta andra för fara.

2. Syfte

Avsikten med policyn är att skydda kommunens informationstillgångar mot alla hot, interna eller externa, såväl avsiktliga eller oavsiktliga samt mot obehörig åtkomst. Information kan förekomma i många olika former – data lagrad i datorer, överförd via nät/fax, tryckt på papper, lagrad på band, CD, USB-minne, telefon eller muntligt framförd.

3. Mål

Åtgärder ska fortlöpande vidtas syftande till att information finns tillgänglig, inte förvanskas, inte heller förkommer eller otillbörligen sprids, samt att lagar och tillämpliga regelverk efterlevs.

Målsättningen med informationssäkerheten är att säkerställa kommunens verksamhet mot avbrott, genom att förebygga och minimera verkan av oönskade händelser.

Samtliga delar ska vara mätbara samt följas upp.

4. Policy

4.1. Ansvar

- Policyn omfattar all information som hanteras inom kommunens verksamhet, samt i relation med medborgare och leverantör.
- Kommunfullmäktige har godkänt och ställer sig bakom denna Informationssäkerhetspolicy med tillhörande bilaga ”IT-riktlinjer för medarbetare”.
- Alla chefer är direkt ansvariga för att denna policy följs inom sina respektive ansvarsområden.
- Policyn gäller för kommunens samtliga anställda. Det är varje persons ansvar att följa denna policy. Underlåtenhet kan medföra påföljd.
- Kommunens informationssäkerhetssamordnare har det direkta ansvaret för att leda informationssäkerhetsarbetet, sprida kunskap om och att ge råd/-vägledning för dess införande.

4.2. Definition

Utifrån varje verksamhets kravbild ska;

- informationens **tillgänglighet** säkerställas, d.v.s. att informationen finns tillgänglig när den behövs.
- informationens **riktighet** säkerställas, d.v.s. att informationen är korrekt och fullständig.
- informationens **sekretess** säkerställas, d.v.s. att endast behöriga kommer åt informationen.
- informationens **spårbarhet** säkerställas, d.v.s. att man i efterhand kan följa händelser i IT-systemen och koppla dessa till en specifik händelse.

4.3. Planer och analyser

- Systemsäkerhetsplan ska genomföras för alla kritiska verksamhetssystem.
- Förvaltningschef ska upprätta avbrottsplan som ska underhållas och testas.
- Riskanalys ska årligen genomföras för varje kritisk informationstillgång.

4.4. Dokumentation

- Kritiska informationstillgångar ska dokumenteras och tilldelas en ägare.
- Klassificering och värdering av informationstillgångar ska upprätthållas.
- Respektive nämnd ska ta fram riktlinjer och rutiner för sin förvaltning till stöd för denna policy med angivande av ansvarsförhållanden för genomförande och förvaltning.

4.5. Utbildning

Utbildning i informationssäkerhet ska ges alla anställda genom informationssäkerhetssamordnarens omsorg.

4.6. Övrigt

- Gällande lagstiftning och avtal ska uppfyllas.
- Alla säkerhetsincidenter, konstaterade eller misstänkta, ska rapporteras till och undersökas av informationssäkerhetssamordnaren.

Regelbundna revisioner av att policyn efterlevs ska genomföras.

1. Klarläggande

Detta dokument syftar till att utveckla punkterna som anges i informationssäkerhetspolicyn för Vänersborgs kommun. Dokumentet är inte en fortsättning på policyn utan mer en hjälp för att förstå konsekvensen av policyns innehåll.

1.1. Definition av Informations- och IT-säkerhet

Med begreppet informationssäkerhet avses säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla fastställda krav avseende *sekretess, riktighet, tillgänglighet och spårbarhet*.

Med begreppet IT-säkerhet avses säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation.

1.2. Målet med kommunens informationssäkerhetsarbete

Inom Vänersborgs kommun är informationsbehandlingen omfattande. Den har strategisk betydelse för kommunens verksamhet och för den nivå på service som kommunen tillhandahåller sina medborgare. Information är en viktig tillgång varför den måste skyddas mot förlust, förvanskning, obehörigt nyttjande etc. Vänersborgs kommun är samlingsbegreppet för all verksamhet som bedrivs av enheter där Vänersborgs kommun har avgörande ägarinflytande.

Information återfinns i många olika former, t.ex. i brev som inkommer till kommunen, i handlingar som upprättas, i IT-system, i samtal och diskussioner o.s.v. De skyddsmetoder som erfordras inkluderar bl.a. riktlinjer, rutiner, organisation, säkerhetstekniska lösningar och ett gott säkerhetsmedvetande.

Informationssäkerhetsarbetet och skyddet omfattar all den information, oavsett om IT-stöd nyttjas eller inte, som hanteras, lagras, bearbetas etc. inom kommunen. Informationsskyddet måste möta de krav som ställs i gällande lagstiftning, av medborgarna, den egna verksamheten etc. Skyddet skall vara utformat så att tillgången till information och öppenheten inom kommunens verksamheter förblir så stor som möjligt för allmänheten.

Aktuellt skydd skall alltid kunna hänföras till ställda skyddskrav, vilka även skall ta hänsyn till aktuell hot- och riskbild. Det är av vikt att aktuella hot- och risker mot informationen, dess hantering och dess behandling, kartläggs hos respektive verksamhet inom kommunen för att möjliggöra införandet av ett effektivt och adekvat informationsskydd. Kommunens informationssäkerhetsskydd utgörs av den samlade effekten av de skyddsåtgärder som reducerar risken för att hot utfaller gentemot informationens sekretess, riktighet, tillgänglighet och åtgärder som reducerar de negativa konsekvenserna om ett hot utfaller.

1.3. Styrande dokument för kommunens informationssäkerhet

Inom kommunen är det ett flertal olika regelverk som styr vilka regler som är gällande avseende information, dess hantering och behandling. Föreligger motsägelser i de olika regelverken är det **alltid** gällande lagstiftning som skall följas. Följande hierarki avseende reglerna för informationssäkerheten inom kommunen är gällande.

1. Gällande lagstiftning och andra relevanta/tvingande regelverk.
2. Regler kring informationssäkerhet utfärdade av kommunens informationssäkerhetssamordnare.
3. Regler kring nyttjande av IT-säkerhetstekniska lösningar utfärdade av IT-avdelningen.
4. Regler kring informationssäkerhet utfärdade av nämnder/styrelser.
5. Regler kring informationssäkerhet utfärdade av förvaltningschefer eller motsvarande.
6. Regler kring informationssäkerhet utfärdade av informationssäkerhetsombud och IT-säkerhetssamordnare.
7. Regler kring informationssäkerhet utfärdade av informationssystemägare.
8. Handhavandeinstruktioner och användarinstruktioner.

Informations- och IT-säkerheten skall så långt som möjligt integreras i de rutiner som gäller för den specifika informationshanteringen/ informationssystemet.

1.4. Organisation och ansvar

Kommunens informationssäkerhetsarbete bygger på att den som ansvarar för en verksamhet därmed även ansvarar för verksamhetens informationssäkerhetsskydd. Ansvaret för att erforderligt skydd införs, förvaltas och vidareutvecklas åvilar alltid verksamhetsansvariga.

1.4.1. Kommunfullmäktige

Kommunfullmäktige fastställer kommunens informationssäkerhetspolicy enligt vilken kommunens informationssäkerhetsarbete skall bedrivas och organiseras och är ytterst ansvarig för att en god säkerhet finns och upprätthålls inom kommunen och dess verksamheter.

1.4.2. Kommunchefen

Kommunchefen utser kommunens informationssäkerhetssamordnare.

1.4.3. Informationssäkerhetssamordnare

Kommunens informationssäkerhetssamordnare är direkt underställd kommunchefen och ansvarar för

- upprättande, vidareutveckling och förvaltning av kommunens övergripande informationssäkerhetsregler,
- upprättande av utbildningsmaterial i kommunens övergripande informationssäkerhetsregelverk,
- framtagande av metodstöd etc. inom informationssäkerhetsområdet,
- en årlig sammanställning av informationssäkerhetsincidenter inom kommunen, med incident avses händelse som potentiellt kan få eller kunnat få allvarliga konsekvenser för verksamheten,
- att upprätthålla en aktuell övergripande hot-/riskbild mot kommunens informationsförsörjning,

samt

- har befogenhet att stoppa sådan verksamhet som bryter mot gällande regelverk för informationssäkerhet,
- kan utfärda dispenser till förvaltningar och bolag att avvika från kommunens gällande regelverk (dock inte kommunens informationssäkerhetspolicy) kring informationssäkerhet under förutsättning att förvaltningen och nämndens ledning accepterat den ökade hot/riskexponeringen. Dispenser skall vara tidsbegränsade och omfattar normalt en giltighetstid om 3 månader men i särskilda fall upp till 12 månader,
- utgör kontaktperson gentemot andra organisationer,
- utgör expertstöd till kommunens förvaltningar och bolag i informationssäkerhetsfrågor.

1.4.4. Förvaltnings- och bolagschefer (nämnder och styrelser)

Nämnder och styrelser är ytterst ansvariga för att informationssäkerheten möter aktuell hot-/riskbild mot verksamheten. Förvaltnings- och bolagschefer har normalt av nämnd/styrelse delegerats att operativt ansvara för informations- och IT-säkerheten inom verksamheten.

En chefsbefattning innebär säkerhetsansvar och ansvar för att personalen är informerad om gällande policy (säkerhetspolicy och informationssäkerhetspolicy), regler och tillhörande bilaga ”IT-riktlinjer för medarbetare” samt att dessa följs inom ramen för ansvarsområdet.

Respektive chef ansvarar för att rapportering av incidenter, utan fördröjning, sker till informationssäkerhetssamordnaren.

1.4.5. IT-chef

IT-avdelningen äger kommungemensamma informations- och IT-säkerhetslösningar samt har befogenhet att utfärda anvisningar om att specifika IT-säkerhetstekniska lösningar skall användas inom kommunen om de uppfyller verksamhetens krav på informationssäkerhet.

IT-chef ansvarar för att

- tillhandahålla en teknisk driftmiljö som motsvara de av systemägaren ställda krav, som gäller tillgänglighet av informationen. Dessa krav definieras i systemsäkerhetsplanen för systemet
- IT-säkerheten möter de krav som ställs
- upprätthålla en aktuell hot-/riskbild mot IT-verksamheten
- utgöra expertstöd till verksamheten i IT-säkerhetsfrågor
- rapportering av incidenter, utan fördröjning, sker till säkerhetssamordnaren
- riktlinjer, användarinstruktioner, installationsanvisningar etc. innehåller erforderlig information kring IT-säkerhet
- uppdatera bilagan till denna policy, ”IT-riktlinjer för medarbetare”

1.4.6. Systemägare

Med system avses såväl manuella rutiner såväl som rutiner som helt eller delvis utgörs av IT-stöd. Systemägarna ansvarar för att informations- och IT-säkerheten möter de krav som ställs, genom att upprätta en systemsäkerhetsplan samt en aktuell hot-/riskbild för de system som av kommunen är klassade som kritiska.

Systemägaren ansvarar även för att en hot-/riskanalys utförs på systemet samt att erforderligt skydd utifrån systemsäkerhetsplanens krav införs innan driftsättning. Dessa krav gäller även vid förändring av driftsatt system. En årlig uppdatering av systemsäkerhetsplan samt en hot-/riskanalys skall genomföras på driftsatta system.

1.4.7. Personal

Kommunens personal skall känna till informationssäkerhetspolicyn samt tillhörande bilaga ”IT-riktlinjer för medarbetare”. Detta ska ställas i relation till den information som hanteras samt de eventuella specifika regler som är gällande inom kommunen.

1.4.8. Externt engagerad personal och extern tjänsteleverantör

Externt engagerad personal och externa tjänsteleverantörer skall ha tagit del av de regler som är relevanta för deras uppdrag innan de får hantera kommunens informationssystem och informationsresurser.

1.5. Uppföljning

Enligt gällande säkerhetspolicy skall uppföljning ske av att säkerhetsnivån är acceptabel inom kommunens förvaltningar och bolag genom säkerhetsrevision i form av intern kontroll. Resultatet av genomförd revision rapporteras till nämnd/styrelse. Säkerhetsrevisionen skall bl.a. mäta antalet inträffade skador, dess omfattning och kostnader samt antalet incidenter, d.v.s. händelser som skulle ha kunnat resultera i en skada. En viktig del i säkerhetsrevisionen är att bedöma kostnaderna i relation till ett ökat säkerhetsskydd.