Kommunal Författningssamling

Informationssäkerhetsstrategi

Dokumenttyp	Strategi
Dokumentnamn	Informationssäkerhetsstrategi
Nämnd	Kommunstyrelsen
Sektor	Styrning och stöd
Antagen	Kommunstyrelsen, 2019-11-20
Paragraf	Ks § 212/2019
Ansvar	Säkerhetschef

KS § 212/2019
2019-11-20

Informationssäkerhetsstrategi för Kävlinge kommun

1. Inledning

Information förekommer i många former. Den kan vara tryckt på papper, elektroniskt distribuerad eller lagrad, överförd via e-post eller meddelandeprogram, visas på film eller video eller rent av yttras i en konversation. Oavsett hur informationen lagras, överförs eller presenteras ska informationen hanteras säkert.

Med *säker hantering av information* menas att informationen aktivt skyddas från oacceptabla risker, som kan leda till exempelvis ofrivillig förlust eller läckage av information. Den säkra hanteringen inriktar därmed informationssäkerhetsarbetet mot att i huvudsak identifiera, bedöma och värdera risker samt hantera de risker som bedöms som oacceptabla. Men för att kunna bedriva ett fungerande säkerhetsarbete kring kommunens informationstillgångar behövs tydliga riktlinjer. Kävlinge kommuns informationssäkerhetsstrategi har därför tagits fram för att förtydliga kommunens viljeriktning med det praktiska informationssäkerhetsarbetet.

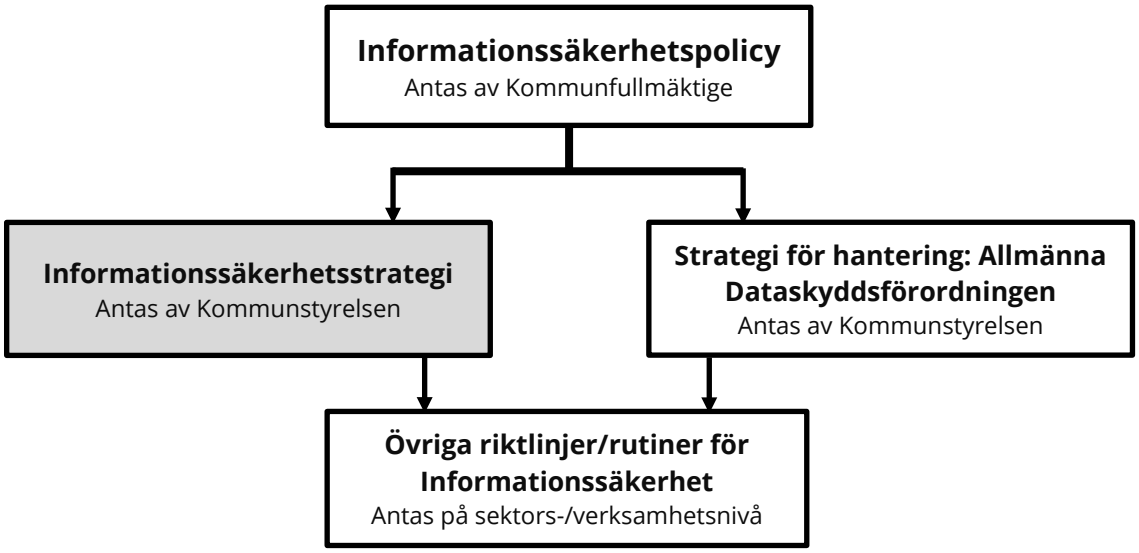
1.1 Informationssäkerhetsstrategins förhållande till övriga informationssäkerhetsdokument

Kävlinge kommuns informationssäkerhetsstrategi är en konkretisering av Kävlinge kommuns informationssäkerhetpolicy, och syftar till att lyfta fram ledningens ambitionsnivå inom de områden som normalt räknas in i informationssäkerheten. Ambitionsnivån ska spegla gällande lagstiftning, samt de arbetssätt som är unika för Kävlinge kommuns och de informationstillgångar som används där.

Det praktiska och dagliga informationssäkerhetsarbetet konkretiseras sedan ytterligare i sektors-/verksamhetsspecifika riktlinjer och rutiner avseende informationssäkerhet. Dessutom finns ett kommunövergripande stöddokument kallat *Handbok för informationssäkerhet*, som på ett så detaljerat som möjligt beskriver hur olika former av information ska hanteras, i enlighet med ledningens ambitionsnivå, gällande lagstiftning, Myndigheten för Samhällsskydd och Beredskaps rekommendationer samt den etablerade svenska och internationella standarden inom området, *SS-ISO/IEC 27000*.

Informationssäkerhetspolicyn och informationssäkerhetsstrategin tillsammans med *Handbok för informationssäkerhet* ska tillämpas av alla som deltar i kommunens verksamheter; det vill säga såväl anställa, praktikanter, konsulter som leverantörer, med flera.

Se följande illustration för att få en tydlig bild över hur Kävlinge kommuns informationssäkerhetsarbete är uppbyggt utifrån ett styrnings- och ledningsperspektiv:



1.2 Begrepp inom informationssäkerheten

Begrepp och definitioner för informationssäkerhetsarbetet framgår av *Handbok för informationssäkerhet* och gäller för alla kommunens verksamheter.

2. Syfte med Kävlinge kommuns informationssäkerhetsarbete

Syftet med denna informationssäkerhetsstrategi är att, tillsammans med kommunens *Informationssäkerhetspolicy* och *Handbok för informationssäkerhet*, säkerställa ett genomgående systematiskt och effektivt informationssäkerhetsarbete på alla nivåer i kommunen.

Syftet är också att belysa vilket ansvar verksamheterna och dess anställda har i förhållande till gällande lagstiftningar, samt att lägga grunden för verksamheternas egna rutiner och riktlinjer kopplade till informationssäkerhet.

3. Mål med Kävlinge kommuns informationssäkerhetsarbete

Den övergripande informationssäkerhetspolicyn efterlevs genom *att*:

- Etablera ett systematiskt arbetssätt med entydiga definitioner, metodik och kravhantering med stöd av *SS-EN ISO/IEC 27000*
- Styra arbetet genom ett kommunicerat och allmänt känt regelverk. Detta innebär också att all personal, konsulter och leverantörer ska ha kunskap om de informationssäkerhetsregler som gäller för dem i deras verksamhet
- Kommunicera en korrekt och konsekvent roll- och ansvarsfördelning avseende kommunens informationstillgångar
- Kommunens informationstillgångar ska vara väl tillgängliga för dess verksamheter och informationsförsörjningen ska vara effektiv och säker
- All personal, konsulter och leverantörer ska ha korrekt tillgång till de informationstillgångar som de behöver för att kunna utföra sitt arbete på bästa sätt

- Kravbilden för varje enskilt informationssystem som bedöms vara av stor vikt för kommunens verksamhet ska registreras, klassificeras, kravhanteras och riskhanteras
- Krishanteringsförmågan och kontinuiteten i verksamheterna ska kunna upprätthållas
- Ingångna avtal ska vara kända och följas
- Det ska finnas en gemensam, säker och väldefinierad infrastruktur för intern och extern datakommunikation. Detta gäller också för hanteringen av informationssäkerhetsincidenter och -brister

5. Organisation för Kävlinge kommuns informationssäkerhetsarbete

Kommunfullmäktige har det övergripande ansvaret för kommunens policys, vilket innefattar informationssäkerhetspolicyn. Det är dock kommunstyrelsen som ansvarar för att besluta om och revidera informationssäkerhetsstrategin (detta dokument), samt för att *strategiskt* övervaka nämndernas arbete. Varje nämnd med tillhörande sektor/verksamheter ansvarar i sin tur för det *praktiska* informationssäkerhetsarbetet, vilket innefattar att efterleva de krav och ambitionsnivåer som fastslås av kommunfullmäktige och kommunstyrelsen. Nämnderna och deras verksamheter (högsta chefer) har *alltid* det yttersta svaret för att informationssäkerheten upprätthålls hos dem och deras verksamheter.

Säkerhetsenheten är kommunens övergripande strategiskt ansvariga enhet för informationssäkerhetsarbetet, och ska därför agera samordnande och vägledande mot verksamheternas praktiska informationssäkerhetsarbete. Säkerhetsenheten har dock inget ansvar att *säkerställa* att kommunens verksamheter efterlever de lagkrav som finns avseende verksamhetens informationshantering, utan detta ansvar har verksamheterna (nämnden) själv. Säkerhetsenheten har heller inget ansvar att *säkerställa* att varje enskild anställd uppfyller de krav som finns avseende informationssäkerhet, utan den anställda måste själv – utifrån säkerhetsenhetens övergripande arbete – tillgodose sig med tillräcklig information för att kunna efterleva de informationssäkerhetskrav som finns i den anställdas verksamhet.

Varje nämnd ska utse minst en informationssäkerhetssamordnare (utpekad anställd), som har ett extra ansvar gentemot nämndens verksamheter och som vid behov kan ta fram/revidera verksamhetsspecifika riktlinjer/rutiner kopplat till informationssäkerhet, liksom samverka med övriga informationssäkerhetssamordnare där detta anses lämpligt.

Extern kontakt med Datainspektionen, Myndigheten för samhällsskydd och beredskap samt Säkerhetspolisen ska genomföras enlig gällande lagstiftning och förordning.

6. Personalsäkerhet

Före anställning, praktiktjänstgöring, konsultuppdrag eller beslut om leverantörsavtal ska verifiering av adekvat kompetens och erfarenhet göras.

All personal ska genomföra en grundläggande informationssäkerhetsutbildning som bland annat omfattar hotbild, det interna regelverket samt eget ansvar för informationssäkerhet, inklusive eventuell rollbaserad utbildning i systemstöd för informationssäkerhetsarbetet.

Personal, konsulter med flera som deltar i säkerhetskänslig verksamhet ska placeras i säkerhetsklass. Säkerhetsprövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas.

7. Hantering av informationstillgångar

Nedan presenteras övergripande hur kommunens digitala och fysiska informationstillgångar ska hanteras. Verktyg (fysiska, digitala) som används för att hantera kommunens informationstillgångar ska *alltid* hanteras/användas med hänsyn till informationens art och känslighet. Detaljer presenteras i *Handbok för informationssäkerhet*.

7.1 Informationssystem

Nämnder, sektors-, och verksamhetschefer som fattar beslut om anskaffning, utveckling och avveckling av informationssystem är juridisk ansvariga systemägare (enskilt eller solidariskt).

Systemägare ska utse ansvarig systemförvaltare (och eventuellt systemadministratörer), vilken ansvarar för den dagliga (operativa) användningen av informationssystemet, att säkerhetskrav efterlevs genom kravhantering samt att systemet stödjer verksamheten enligt en vedertagen systemförvaltningsmodell.

Ägare av informationssystem är också ägare till de integrationer som beställts och implementerats för informationsinformationssystemets aktuella funktion.

Alla informationssystem samt personuppgiftsbehandlingar ska dokumenteras. Informationssystem ska även klassificeras, kravhanteras och riskhanteras.

Beroenden mellan informationssystem samt beroende av IT-tjänster ska klassificeras. IT-tjänsternas inbördes behov av IT-system och IT-infrastruktur ska dokumenteras.

Risker i Informationssystem, personuppgiftsbehandling och stödjande processer som riskbedöms över kommunens riskacceptansnivå ska hanteras.

Informationssystem som hanterar/innehåller sekretessbelagd/känslig information[1] ska kunna upprätthålla adekvat säkerhetsnivå sett till den sekretessbelagda/känsliga informationen, samt tydligt kunna markera att viss information är skyddad med sekretess

Informationssystem och personuppgiftsbehandlingar får enbart användas för de ändamål de ursprungligen och uttryckligen är avsedda för.

Lagringsmedia som byts ut eller ersätts för informationssystem och skrivare som hanterar sekretessbelagd-, säkerhetsklassad- eller integritetskänslig information/data ska förstöras enligt en förutbestämd destrueringsrutin.

7.2 Fysiska handlingar/dokument

Utskrifter från system som innehåller sekretessbelagd/känslig information (även personuppgifter) ska:

- enbart ske från åtkomstskyddade skrivare (autentisering krävs)
- märkas med aktuell säkerhetsklassificering eller motsvarande
- förvaras i säkert utrymme när de ej används/hanteras

Säkerhetsskyddsklassificerade handlingar ska förses med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har.

Säkerhetsskyddsklassificerad handling *Kvalificerat hemlig* ska inventeras minst en gång per år.

---

[1] *Enligt Offentlighets- och sekretesslagen, Lag om behandling av personuppgifter inom socialtjänsten, Dataskyddsförordningen (GDPR), Patentdatalagen, med flera.*

8. Styrning av åtkomst

Åtkomst till information inom kommunen ska baseras på användaridentitet, användarroll samt informationens/informationsinformationssystemets klassificering. Utöver detta bör faktorer som klient, tid på dygnet, plats med mera beaktas för att styra åtkomst till känslig information.

Grundläggande för all åtkomst till IT-stöd, oavsett form, är att användaren ska ha ett unikt användarnamn samt att användaren kan autentisera sig med minst ett kvalificerat lösenord[2].

För åtkomst till sekretessklassad eller på annat sätt känslig/integritetskänslig information[3] över öppna eller osäkra nät ska förstärkt autentisering i form av tvåfaktorsautentisering användas.

Åtkomst till information/informationssystem som innehåller säkerhetsklassad information får ej ske över nätanslutning, utan får enbart ske mot en intern tillträdeskontrollerad fristående station (maskin) och av en autentiserad användare.

9. Kryptering/begränsning av information

Krypteringssystem och liknande tekniker bör utnyttjas för att skydda information som anses vara utsatt för risk och för vilken andra åtgärder inte ger tillräckligt skydd.

Kommunikation av säkerhetsklassad information får enbart ske enligt aktuell myndighets bestämmande.

Regler för användning, skydd och giltighetstid för kryptografiska nycklar för deras hela livscykel ska utvecklas och införas i den mån kryptering används.

10. Fysisk och miljörelaterad säkerhet

Tillträde till kontor och utrymmen där informationsbehandlingsresurser av viktig/känslig karaktär kan nås ska begränsas till behörig personal.

Utrustning, information eller program med viktig/känslig information får inte avlägsnas från verksamhetens lokaler utan särskilt tillstånd av sektors- eller verksamhetschef.

Server och systemdrift ska bedrivas i utrymmen som är avsedda för detta ändamål och försedda med nödvändigt brandskydd, fukt-, och temperaturreglering, avbrottsfri kraftförsörjning, larm samt tillträdeskontroll, allt enligt vedertagen branschstandard.

11. Driftsäkerhet

Enbart av kommunens IT-avdelning godkänd utrustning får anslutas till kommunens interna nätverk.

Informationssystemens/-tjänsternas behov av skydd ska baseras på aktuell informationssäkerhetsklassificering. Systemägarens möjlighet till kontroll och uppföljning av aktuellt skydd ska beaktas särskilt.

Informationssystem och viktiga IT-komponenters driftplats, oavsett om det är en intern eller extern tjänst, ska också avgöras utifrån informationssäkerhetsklassificeringen.

Verksamhetens behov av datakommunikation och drift av informationssystem och IT-tjänster ska framgå av ett särskilt servicenivåavtal (SLA) mellan aktuell systemägare och IT-driftansvarig. Detta

---

[2] *Med kvalificerat lösenord avses minst åtta (8) tecken som innehåller stora och små bokstäver, siffror och specialtecken.*

[3] *Enligt Offentlighets- och sekretesslagen, Lag om behandling av personuppgifter inom socialtjänsten, Dataskyddsförordningen (GDPR), Patentdatalagen, med flera.*

ska omfatta såväl servicenivåkrav (tillgänglighet, support etc.) som säkerhetskrav (anslutningar, backup, återställning, kryptering etc.). Dessa krav ska bygga på informationssystemets/-tjänstens klassificering.

Driftleverantör ska ha funktioner och tillgänglig planering och kompetens för att återställa driftmiljön inom ramen för de aktuella servicenivåavtalen (SLA), bland annat genom att implementera avbrottsfri kraft för automatisk ordnad nedstängning vid elavbrott tillsammans med övriga adekvata återställningsrutiner (enligt branschstandard).

Alla ändringar i IT-driftmiljön (inklusive ändringar i informationssystem/applikationer/tjänster, med mera) ska beställas genom en formell ändringsbeställning som tillhandahålls av driftleverantören.

Ändringsärende som kan beröra flera organisationsdelar och många användare eller tillgångar med höga tillgänglighetskrav ska föregås av en risk- och konsekvensbedömning med representanter ifrån alla berörda parter.

12. Kommunikationssäkerhet

Kommunikation som innehåller sekretessbelagd/känslig information[4] ska krypteras eller likvärdigt över öppna eller osäkra nät.

Sekretessbelagd och integritetskänslig information ska skyddas oavsett om den presenteras, transporteras eller är i vila (lagrad).

13. Anskaffning, utveckling och underhåll av system

Nyanskaffning, utveckling eller avveckling av informationssystem ska genomföras enligt en organisationsövergripande fastställd modell/metod. Detta gäller även för informationstjänster och systemstöd som avtalas som tjänst (exempelvis molntjänster). Modellen/metoden ska även omfatta säkerhetskrav.

Ägaren (beställare) är den som fattar beslut om anskaffning/produktionssättning och ska fatta beslut om anskaffning och produktionssättning i samråd med IT-leverantör och i enlighet med informationssäkerhetspolicyn, detta dokument samt krav och risker från klassificering och riskanalys.

14. Leverantörer av informationssystem

Leverantörer som har/får tillgång till personuppgifter ska regleras genom ett *personuppgiftsbiträdesavtal.* Leverantörer som har/får tillgång till annan typ av säkerhetskänslig information ska regleras genom någon form av säkerhetsavtal/säkerhetsöverenskommelse.

Säkerhetsklassad information får ej lämnas ut till utländsk leverantör såvida inte Sverige ingått en överenskommelse om säkerhetsskydd med den andra staten och leverantören har godkänts genom en kontroll enligt den andra statens säkerhetsskyddslagstiftning.

15. Hantering av informationssäkerhetsincidenter

Incidentrapportering avseende negativa händelser i informationssystem/tjänster ska utformas så att systemägaren/personuppgiftsansvarig automatiskt delges incidentrapporten (eller kopia av rapporten) oavsett hur rapporteringskedjan är utformad från källan och vidare.

---

[4] Enligt Offentlighets- och sekretesslagen, Lag om behandling av personuppgifter inom socialtjänsten, Dataskyddsförordningen (GDPR), Patentdatalagen, med flera.

Övrig incidentrapportering och anmälan ska ske enligt *Handbok för informationssäkerhet* till antingen Datainspektionen (DI), Myndigheten för samhällsskydd och beredskap (MSB), eller Säkerhetspolisen (SÄPO) beroende på vad incidenten gäller.

Om en säkerhetshotande händelse har inneburit en förlust av säkerhetsskyddsklassificerade uppgifter eller att uppgifterna kan ha röjts, ska verksamhetsutövaren snarast, dock senast i samband med att en anmälan om detta görs till Säkerhetspolisen, påbörja arbetet med en skadebedömning.

Verksamhetsutövaren ska snarast, dock senast i samband med att en anmälan om en säkerhetshotande händelse görs till Säkerhetspolisen, överväga behovet av att informera andra verksamhetsutövare som från säkerhetsskyddssynpunkt kan vara berörda av händelsen.

16. Hantering av verksamhetens kontinuitet

Sektorernas ledningsgrupper ansvarar för att identifiera sektorns kritiska verksamheter och att lägsta servicenivå fastställs för dessa verksamheter i händelse av avbrott/störningar. Detta arbete ska ske med stöd av säkerhetsenheten.

De identifierade verksamheterna som stöds av informationssystem ska utforma en reservrutin för att kunna vidmakthålla lägsta servicenivå vid avbrott/störning i systemleveransen.

Verksamhetens kontinuitetsplanering ska även omfatta IT-relaterade hot och risker. I detta ingår att beskriva konsekvenser vid avbrott i viktiga/känsliga informationssystem i syfte att skapa underlag för återställningsplaner (IT-driftleverantör) och IT-kontinuitetsplan.

Verksamhetens kontinuitetsplan ska beskriva hur verksamheten förbereder och genomför identifierad kritisk verksamhet på en lägsta servicenivå över en bestämd tidsperiod.

För kritiska Informationssystem ska en återställningsplan för informationssystemet finnas som tas fram av ansvarig verksamhet tillsammans med driftleverantör eller motsvarande.

En IT-kontinuitetsplan som stödjer alla verksamheters kontinuitetsplaner med IT-tekniska lösningar, baserad på gällande servicenivåavtal (SLA) och konsekvensanalys ska upprättas och vidmakthållas genom IT-driftansvarigs försorg.

Reservrutiner, kontinuitetsplaner för verksamheten och IT-kontinuitet ska harmoniseras i ett övergripande ramverk för kontinuitetsplanering inom kommunen. Härvid ska även harmonisering med aktuell risk- och sårbarhetsanalys samt krisplanering beaktas.

17. Efterlevnad/Uppföljning av arbetet

Varje nämnd, sektor och verksamhet ansvarar enskilt för att identifiera och uppfylla de lagar och förordningar med mera som respektive verksamhet styrs/påverkas av. Kommunstyrelsen (säkerhetsenheten) har dock en övergripande samordnings- och uppföljningsroll. Det är även säkerhetsenheten som ansvarar för att vid behov (men minst en gång vart femte år) revidera kommunens övergripande informationssäkerhetsdokument (informationssäkerhetspolicy, informationssäkerhetsstrategi, *Strategi för hantering: allmänna dataskyddsförordningen*, samt *Handbok för informationssäkerhet*). De sektors-/verksamhetsspecifika informationssäkerhetsrutiner och -riktlinjer som tas fram ansvarar varje sektor enskilt för att revidera enligt egenbeslutade intervall.

Klassificeringar av system/tjänster/behandlingar ska följas upp minst en gång vartannat år. Ansvarig för detta arbete är systemförvaltaren, eller den systemförvaltaren utser. Krav som identifierats genom klassificeringen och som ändras (sänks eller höjs) samt riskbedömningar med riskvärden över riskacceptansnivå är *avvikelser* som ska kontrolleras och följas upp av systemägaren så snart de upptäcks.

Teknisk kontroll av systemen ska utföras med jämna mellanrum. Dessa kontroller syftar till att undersöka att implementerade säkerhetslösningar är korrekta. I detta arbete ingår också i tillämpliga fall att utföra legala intrångsförsök för att undersöka hur effektiva de skydd är som verksamheten valt. Hur ofta och hur omfattande en teknisk kontroll ska göras/genomföras ska regleras i någon form av avtal, överenskommelse eller rutin.