Riktlinje för informationssäkerhet

I Linköpings kommun

Dokumenttyp: Riktlinje
Antaget av: Kommunstyrelsen 2019-11-19, § 359
Senast reviderat: - Förslag Kommunstyrelsen 2025-06-10, §, Kommunstyrelsen 2021-04-20, § 118
Giltighetstid: Gäller tills vidare

Diarienummer: KS 2025-431
Dokumentansvarig: Kommundirektören
Adresserat till: Samtliga nämnder
Tidpunkt för aktualitetsprövning:
Relaterade styrdokument: Säkerhetspolicy, Kommunövergripande tillämpningsanvisning till riktlinje för informationssäkerhet.>
Sökord: LIS, Informationssäkerhet, Info Säk

Innehåll

1. Inledning

1.1 Bakgrund

Det ställs allt högre krav på kommunens arbete med informationssäkerhet. Denna riktlinje syftar till att, med särskilt fokus på regulatorisk efterlevnad, konkretisera säkerhetspolicyn vad avser informationssäkerhetsarbetet i kommunens nämnder (i detta ingår kommunstyrelsen). Kommunstyrelsen ska, med stöd av denna riktlinje, styra nämndernas informationssäkerhetsarbete. Riktlinjen innehåller bland annat ansvar, roller och mål för informationssäkerhetsarbetet.

1.2 Omfattning och avgränsning

Den primära målgruppen för denna riktlinje är de tjänstepersoner som har en särskild roll i kommunens informationssäkerhetsarbete men den gäller för samtliga användare, medarbetare och förtroendevalda i kommunen. Den gäller även för medarbetare hos externa aktörer[1], exempelvis inhyrda konsulter, entreprenörer, organisationer och andra som på olika sätt hanterar kommunens information. När begreppet medarbetare används i texten gäller det samtliga ovanstående roller.

Den verksamhet och informationshantering som träffas av säkerhetsskyddslagen (informationsklass 4) omfattas inte av kraven i denna riktlinje. För sådan hantering gäller säkerhetsskyddslagen med därtill hörande föreskrifter samt andra styrdokument som kommunen beslutat om.

2. Informationssäkerhetsarbete

2.1 Informationssäkerhet

För att kommunen ska kunna genomföra den planerade digitaliseringen med en acceptabel risknivå är en god informationssäkerhet en förutsättning.

I enlighet med säkerhetspolicyn är informationssäkerhet kommunens förmåga att hantera informationen så att legala, etiska, och verksamhetsmässiga intentioner upprätthålls. Informationssäkerhet innebär att rätt information finns tillgänglig för rätt mottagare vid rätt tidpunkt. I kommunen består informationssäkerhet av två delar: administrativ säkerhet och teknisk säkerhet. Med teknisk säkerhet avses IT-säkerhet och fysisk säkerhet. Informationssäkerhet handlar om att skapa och upprätthålla ett lämpligt skydd av information. Information behöver försvaras mot de hot den utsätts för. Information kan till exempel finnas i och hanteras med stöd av IT-system, på papper eller direkt av människor i

[1] Personer från dessa verksamheter kan också betecknas uppdragstagare. För att någon ska anses vara uppdragstagare i offentlighets- och sekretesslagens mening krävs att uppdraget ges direkt till en fysisk person. Uppdragstagaren har inte rätt att sätta någon annan i sitt ställe. Uppdragstagaren är normalt så knuten till myndigheten att hen kan sägas delta i myndighetens egentliga verksamhet, det vill säga som regel myndighetens uppgifter enligt instruktion eller motsvarande reglering.

form av tal. IT-säkerhet fokuserar på säkerhet i datorer och datornätverk medan informationssäkerhet omfattar all information oavsett form.

Nämnderna ska säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat genom att:

- klassa sin information utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning),
- identifiera, analysera och värdera risker för sin information (riskbedömning),
- utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella skyddsåtgärder, och
- utvärdera skyddsåtgärderna samt vid behov anpassa skyddet av informationen.

Informationssäkerhetsarbetet och införda skyddsåtgärder ska dokumenteras.

Kommunen eftersträvar att informationssäkerhetsarbetet inom nämnderna ska följa de internationella standarderna SS-ISO/IEC 27001/2[2].

2.2 Informationssäkerhetskultur

För att informationssäkerhetsarbetet ska lyckas behövs en god informationssäkerhetskultur inom kommunen. Detta innebär förenklat att alla medarbetare, genom att prioritera och agera på rätt sätt, bidrar till att vidmakthålla kommunens informationssäkerhet. Grunden för en god informationssäkerhet är att alla medarbetare ska ha nödvändig kunskap för att kunna och vilja agera rätt, samt att kommunens system och säkerhetslösningar gör det lätt att göra rätt.

2.3 Ledningssystem för informationssäkerhet

Linköpings kommuns ledningssystem för informationssäkerhet (LIS) är en del av kommunens totala ledningssystem för hur kommunen planerar, genomför, kontrollerar, följer upp, utvärderar och förbättrar sin verksamhet. Ledningssystemet för informationssäkerhet har emellertid ett särskilt fokus på processer för styrning och ledning av informationssäkerhetsarbetet. Dessa processer ska utvärderas löpande och anpassas till aktuella verksamhets- och omvärldskrav. Ledningssystemet för informationssäkerhet utgår från Reglementet för Linköpings kommun och säkerhetspolicyn samt kompletteras och konkretiseras i ytterligare styrdokument såsom denna riktlinje, tillämpningsanvisningar, regler och rutiner. Därtill utgör kommunens styr- och samverkansmodell för digitalisering med tillhörande styrdokument en väsentlig förutsättning för en stor del av det praktiska arbetet som sker inom objektorganisationen.

2.4 Informationsklassning

Informationsklassning ska genomföras för all kommunens information för att därefter kunna tilldela informationen lämpligt skydd. Samtliga bedömningar av skyddsbehov för information

[2] Ledningssystem för informationssäkerhet och Informationssäkerhetsåtgärder.

ska göras enligt kommunens modell för informationsklassning. Modellen består av fem skyddsnivåer (nivå 0-4). Nivå 4 gäller säkerhetsskydd och omfattas inte av denna riktlinje.

Bedömningar av skyddsbehov ska göras utifrån informationssäkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.

Kommunens modell för informationsklassning ska visa vilket skyddsbehov en viss information har. För informationssäkerhetsaspekten konfidentialitet finns en koppling till lagstiftning avseende offentlighet och sekretess, dataskyddsförordningen samt övriga till området hörande lagar. För konfidentialitet, riktighet och tillgänglighet gäller att skyddsbehovet för informationen avgörs genom att sex konsekvensområden värderas: verksamhetens förmåga att utföra sin uppgift, ekonomiska konsekvenser, påverkan på individ, påverkan på externa intressenter, juridiska aspekter och påverkan på kommunens anseende (förtroende/rykte).

För varje konsekvensområde bedöms eventuella konsekvenser av att en viss information inte har relevant skydd, i nivåerna 0-3, där 0 motsvarar lindriga eller försumbara konsekvenser för kommunen, 1 motsvarar måttliga konsekvenser, 2 betydande konsekvenser och 3 allvarliga konsekvenser.

3. Roller och ansvar

3.1 Ansvar för kommunövergripande styrning av informationssäkerhet

Kommunstyrelsen har ansvar för att konkretisera de långsiktiga strategiska informationssäkerhetsmålen som anges i säkerhetspolicyn. Kommunstyrelsen ansvarar även för att leda och samordna informationssäkerhetsfrågor. Kommundirektören har i uppdrag att upprätta och vid behov revidera kommunövergripande tillämpningsanvisningar avseende informationssäkerhet.

3.2 Ansvar för tillämpning av reglerna i nämnder

Nämnderna ansvarar för att det bedrivs ett effektivt och ändamålsenligt informationssäkerhetsarbete i den egna verksamheten utifrån denna riktlinje. Respektive förvaltningschef är informationsägare med ansvar för den egna förvaltningens informationssäkerhetsarbete, om inte nämnden beslutar annat. Informationsägaren ansvarar för den operativa styrningen och uppföljningen av förvaltningens informationssäkerhetsarbete.

3.3 Ansvar för informationen

En förutsättning för att information ska få ett relevant skydd är att det finns ett tydligt ansvar kopplat till informationen. Därför ska en viss typ eller en viss mängd information ha ett tydligt tilldelat ansvar. Inom kommunen är det alltid en nämnd som har det yttersta ansvaret för den information som hanteras i respektive verksamhet.

Grundprincipen när det gäller ansvar för informationssäkerheten är att ansvaret följer det ordinarie verksamhetsansvaret hela vägen från kommunfullmäktige till enskilda chefer och medarbetare. Principen är att den som är formellt ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamheten. En verksamhet kan exempelvis bedrivas i en organisatorisk del (exempelvis en förvaltning eller enhet), ett löpande arbetsflöde (exempelvis en process) eller ett tidsbegränsat arbete (exempelvis ett projekt).

Informationsägaren ska styra och följa upp det systematiska och riskbaserade informationssäkerhetsarbetet. Informationsägaren ska bland annat fastställa verksamhetens krav på informationssäkerhet genom informationsklassning samt fastställa adekvat skyddsnivå. Informationsägarens ansvar för att verkställa nämndens uppdrag kan inte överlämnas. Däremot kan relaterade arbetsuppgifter överlämnas.

Samtliga medarbetare och övriga som denna riktlinje gäller ska följa gällande regler avseende informationssäkerhet och verka för en god säkerhetskultur.

4. Mål för informationssäkerhetsarbetet

För att uppnå den övergripande målsättningen i säkerhetspolicyn har kommunstyrelsen beslutat om följande mål för informationssäkerhetsarbetet.

- Kommunen ska uppfylla de regulatoriska krav som ställs (regulatorisk efterlevnad).
- Kommunen ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete enligt ett dokumenterat ledningssystem för informationssäkerhet (systematiskt och riskbaserat informationssäkerhetsarbete).
- Det ska finnas en förmåga att fatta väl avvägda riskbaserade beslut utifrån verksamhetens behov, IT-miljöns förutsättningar och aktuell hotbild (styrning och ledning).
- Kommunen ska ha en tillräcklig förmåga att upptäcka, motstå och hantera cybersäkerhetsincidenter för att säkerställa att kommunens verksamhet kan genomföras (cyberresiliens).
- Kommunens digitala miljö ska ha en i grunden säker IT-arkitektur, som kompletterad med tekniska och administrativa säkerhetsåtgärder åstadkommer en tillräcklig skyddsnivå för verksamheten (cyberhygien).
- Kommunens medarbetare och leverantörer ska ha tillräckligt god risk- och säkerhetsmedvetenhet för att kunna och vilja utföra sina arbetsuppgifter på ett säkert sätt (informationssäkerhetskultur).