Riktlinje för informationssäkerhet och dataskydd

RIKTLINJE

FALKÖPING KOMMUNEN

Typ av styrdokument	Riktlinje
Beslutsinstans	Kommunstyrelse
Diarienummer	KS 2023/1347
Giltighetstid	Fr.o.m. 2024-03-01 och tills vidare
Dokumentet gäller för	Samtliga nämnder och förvaltningar i kommunen
Fastställd	2024-02-21, § 52
Ersätter	Finns ingen tidigare version av dokumentet
Dokumentansvarig	Information- och dataskyddssamordnare
Tidpunkt för aktualitetsprövning	Vid behov

Innehåll

1. Inledning

Den här riktlinjen syftar till att konkretisera policy för informationssäkerhet och dataskydd samt ge vägledning i hur policyn ska tillämpas. Riktlinjen är ett av de styrdokument som reglerar informationssäkerhets- och dataskyddsarbetet i Falköping kommun.

Riktlinjen gäller för all verksamhet inom kommunen och omfattar alla informationstillgångar som hanteras. Alla anställda, förtroendevalda och extern personal som hanterar information inklusive personuppgifter inom Falköping kommuns verksamheter omfattas av riktlinjen. Vissa funktioner har dock mer specifika uppgifter inom ramen för informationssäkerhets- och dataskyddsarbetet vilket anges i riktlinjen.

Informationssäkerhet handlar om hur man kan hindra känslig information från att hamna i orätta händer. Informationssäkerhetsarbetet och dataskyddsarbetet ska tillsammans enligt dataskyddsförordningen och dataskyddslagen ge grundläggande rättigheter för hur individer kan skyddas.

Förutom policyn och riktlinjen följer även mer detaljerade rutiner kring hur verksamheterna i Falköping kommun ska arbeta med informationssäkerhet och dataskydd.

2. Syfte

Syftet med riktlinjen är att ge vägledning i hur de strategiska målen i policyn för informationssäkerhet och dataskydd ska uppnås. Den beskriver därmed hur arbetet med informationssäkerhet och dataskydd ska organiseras och systematiskt utföras för att kunna förebygga oönskade händelser och i förekommande fall hantera incidenter.

3. Att arbeta systematiskt

Av Falköping kommuns policy för informationssäkerhet och dataskydd framgår att det ska bedrivas ett systematiskt arbete med informationssäkerhet och dataskydd samt ett förebyggande arbete mot oönskade händelser.

Att arbeta systematiskt med informationssäkerhet och dataskydd innebär att arbeta förebyggande och att kontinuerligt anpassa skyddet för information utifrån organisationens behov och risker. Då finns även rätt information tillgänglig för rätt person vid rätt tidpunkt. Informationstillgångar behöver skyddas utifrån sitt skyddsvärde och information ska inte hamna i orätta händer och missbrukas.

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Exempel på information kan vara i form av text, ljud, bilder eller film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Att information är korrekt som kommunen hanterar i relationer med kommuninvånare, företag och organisationer såväl som inom Falköpings kommun utgör en grund för tillit och förtroende.
Perspektivet med informationssäkerhet och dataskydd är en naturlig del vid utformning av våra arbetssätt och en del av vårt dagliga arbete.

3.1 Systematiskt informationssäkerhetsarbete

Metodstödet för Falköpings kommuns informationssäkerhetsarbete utgår från den etablerade standarden ISO 27000 serien som Myndigheten för Samhällsskydd och Beredskap (MSB) rekommenderar. För att säkerställa att informationssäkerhetsarbetet har tillräcklig nivå i Falköpings kommun är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt. Nedanstående fyra områden är viktiga för ett framgångsrikt och hållbart informationssäkerhetsarbete är;

3.1.1 Identifiera och analysera

För att det systematiska informationssäkerhetsarbetet ska fungera måste informationssäkerhetsarbetet anpassas till kommunens olika verksamheter utifrån deras specifika krav.

Resultatet från analyserna ska styra hur informationssäkerhetsarbetet ska utformas och bedrivas samt vilka säkerhetsåtgärder som behöver införas för respektive verksamhet.

3.1.2 Utforma

Utformningen av kommunens och verksamheternas mål, organisation, handlingsplan och klassningsmodell är viktigt för det långsiktiga arbetet med informationssäkerhet för hela kommunen. Mål och handlingsplan kan underlätta informationssäkerhetsarbetet genom att dela in kortsiktiga- och långsiktiga mål som hanteras utifrån analysernas resultat.

Informationsklassning

Kommunens informationstillgångar behöver inventeras, värderas och klassificeras för att få rätt skydd. Klassningsmodellens roll är att skapa en kommunövergripande ram så klassning och skyddsnivåerna sker på ett likvärdigt sätt på informationstillgångarna.

Genom att klassa informationstillgångarna utifrån säkerhetsaspekterna kan skyddet anpassas och säkerställas för varje informationstillgång utifrån informationssäkerhet och dataskydd. Informationsklassningen syftar till att ge kommunens kritiska informationstillgångar tillräckligt skydd för att undvika överskydd och onödiga kostnader.

Kommunens samtliga informationstillgångar ska finnas förtecknade i det systemstöd som också ger en grund för klassificering, värdering och åtgärdsplan utifrån informationssäkerhet och dataskydd.

Kommunen använder klassningsmodell från Sveriges Kommuner och Regioner (SKR) som bygger på den internationella standarden ISO 27000 som också MSB använder. Genom att följa internationella och nationella riktlinjer underlättar kommunen för externa aktörer att värdera informationstillgångarna likvärdigt ur säkerhetsperspektiven tillgänglighet, riktighet och konfidentialitet.

3.1.3. Använda

Det systematiska informationssäkerhetsarbetet ska fungera i det vardagliga arbetet, vilket förutsätter att aktiviteter från handlingsplan och mål efterlevs enligt uppdrag, roller och ansvar. Medarbetare och förtroendevalda utbildas och hanterar informationstillgångarna efter kommunens rutiner som kopplas till riktlinjen för informationssäkerhet och dataskydd.

3.1.4 Följa upp och förbättra

Krav på informationshantering ändras konstant genom teknisk utveckling, förändrade hotbilder och organisationsförändringar.
För att det systematiska informationssäkerhets- och dataskyddsarbetet ska utvecklas och nå framgång behöver arbetet följas upp och rapporteras. Informationssäkerhetssamordnare och dataskyddssamordnare ska minst 1 gång per år rapportera arbetet med informationssäkerhet och dataskydd till kommunstyrelsen och kommunledningsgruppen enligt kommunstyrelsens reglemente och informationssäkerhetspolicyn.

3.2 Systematiskt dataskyddsarbete

Systematiskt dataskydd är att arbeta förebyggande och kontinuerligt med dataskydd i verksamheterna. Genom att låta dataskyddet bli en integrerad del i organisationens olika processer inom styrning, stödfunktioner och kärnverksamhet blir dataskyddet en naturlig del i de olika processerna för att utveckla, förändra och förbättra verksamheterna.

3.2.1 Ledning och styrdokument

Som ett led i det förebyggande arbetet är det av stor vikt att det finns en medvetenhet hos ledningen för vad dataskydd innebär, att det beaktas tidigt och kontinuerligt i de olika processerna och att det aktivt görs prioriteringar för att nödvändiga säkerhetsåtgärder ska kunna vidtas. Det är av stor betydelse att det finns tydliga styrdokument som är kända för berörda medarbetare och förtroendevalda.

3.2.2 Utbildning

För den faktiska efterlevnaden av dataskyddslagstiftningen och de interna styrdokumenten som följer därav är det viktigt att det finns kunskap och medvetenhet bland medarbetare och förtroendevalda. Många personuppgiftsincidenter orsakas av den mänskliga faktorn vilket visar på ett tydligt behov av utbildning som en del av det förebyggande arbetet.

3.2.3 Säkerställa rättslig grund för behandlingen

Innan en ny behandling av personuppgifter påbörjas ska en bedömning alltid göras om det finns en rättslig grund enligt någon av nedanstående punkter.

Avtal: om behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

Rättslig förpliktelse: om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som framgår av lag eller annan författning, av kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning. Den rättsliga förpliktelsen kan exempelvis vara utformad så att det i lag anges att kommunen är skyldig att lämna vissa uppgifter till en annan myndighet eller till en domstol.

Myndighetsutövning och uppgift av allmänt intresse: om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. För att en uppgift ska anses vara av allmänt intresse ska uppgiften ha stöd i lag eller annan författning, i kollektivavtal eller i beslut som har meddelats med stöd av lag eller annan författning. Uppgifter som kommunen ålagts att utföra genom lag (obligatoriska uppgifter) är av allmänt intresse. Kommuner har också en vidsträckt möjlighet att göra frivilliga åtaganden. Sådana frivilliga åtaganden kan också utgöra uppgifter av allmänt intresse.

Grundläggande intresse: Det är tillåtet för en personuppgiftsansvarig att behandla personuppgifter om det är nödvändigt för att rädda den registrerades eller någon annan persons liv. Det kallas att skydda intressen som är av grundläggande betydelse. I huvudsak handlar det om tillfällen när den registrerade inte kan fatta beslut eller lämna samtycke, till exempel om en person är medvetslös.

Samtycke: om den enskilde samtycker till att sådan behandling sker. För att det ska vara lämpligt att stödja en behandling på samtycke måste samtycket vara frivilligt. Med frivilligt menas att den registrerade har ett genuint fritt val och kontroll över sina personuppgifter. Den registrerade får exempelvis inte drabbas av negativa konsekvenser om den inte lämnar sitt samtycke. För att samtycke ska kunna användas som rättslig grund ska maktförhållandet mellan den personuppgiftsansvarige och den registrerade också vara jämlikt. Maktförhållandet anses ofta vara ojämlikt i relationen

mellan myndighet och medborgare samt mellan arbetsgivare och arbetstagare. Se rutin och exempel för hantering av samtycke.

Intresseavvägning: denna rättsliga grund enligt dataskyddsförordningen inte kan användas av myndigheter när de utför sina uppgifter. Innebörden är att personuppgifter får behandlas utan den registrerades samtycke om den personuppgiftsansvariges intressen väger tyngre än den registrerades och om behandlingen är nödvändig för det aktuella ändamålet.

3.2.4 Säkerställa de registrerades rättigheter

Personen som får sina personuppgifter behandlade (den registrerade) av kommunen har ett antal rättigheter enligt dataskyddsförordningen som den personuppgiftsansvarige ska tillgodose i den mån det är möjligt. Rättigheterna är de nedan angivna.

Rätt till information innan personuppgifter börjar behandlas.

Rätt till tillgång (registerutdrag) om huruvida Falköpings kommun behandlar personuppgifter som rör denne och i så fall får tillgång till personuppgifterna.

Rätt till rättelse av felaktiga uppgifter Den enskilde har dessutom rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen.

Rätt till radering (”rätten att bli glömd”). Det finns undantag från rätten till radering om det är nödvändigt att behålla personuppgifterna för att tillgodose andra viktiga rättigheter som till exempel att uppfylla en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Av denna anledning bör det vara ovanligt att radering blir aktuell i offentlig verksamhet.

Dataportabilitet. Att få ut och använda sina personuppgifter på annat håll. Den som har tagit emot personuppgifterna är skyldig att underlätta en sådan överflyttning av personuppgifter. En förutsättning är att denna behandlar personuppgifterna med stöd av ett samtycke från den registrerade eller för att uppfylla ett avtal med den registrerade och det gäller bara sådana personuppgifter som den registrerade själv har lämnat.

Rätt att invända mot och begära begränsning av personuppgiftsbehandlingar i vissa fall. Det gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning.

Rätt att inte bli föremål för automatiserat beslutsfattande. Den enskilde har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande, inbegripet profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar den enskilde. Den personuppgiftsansvarige måste informera de registrerade om att automatiserat beslutsfattande används enligt den generella informationsskyldigheten i dataskyddsförordningen.

Lämna klagomål. Den enskilde kan lämna klagomål som rör en personuppgiftsbehandling till personuppgiftsansvarig, till dataskyddsombudet och Integritetsmyndigheten (IMY).

Falköping kommun har en e-tjänst på kommunens webbsida som den enskilde kan använda för begäran om registerutdrag, rättelse, radering och begränsning. En prövning av den enskildes begäran ska göras. Om begäran nekas helt eller delvis har den registrerade rätten till ett motiverat beslut med överklagandehänvisning. Se rutin för begäran om registerutdrag, rutin för rättelse, radering och begränsning och rutin för information till registrerade.

3.2.5 Säkerhetsbedömningar och åtgärder

Den personuppgiftsansvarige är skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas i verksamheten. I det arbetet ingår att kartlägga och hantera risker samt att ha rutiner för upptäckt och hantering av personuppgiftsincidenter. Vilka säkerhetsåtgärder som är lämpliga beror bland annat på hur känslig behandlingen är, vilka risker som finns och vilka tekniska lösningar som är tillgängliga. Exempel på tekniska säkerhetsåtgärder är inloggning, behörighetsspärrar, brandväggar, kryptering, pseudonymisering, säkerhetskopiering och antivirusskydd. Exempel på organisatoriska säkerhetsåtgärder är tilldelning av åtkomsträttigheter och styrdokument.

Vid behandling av personuppgifter som sannolikt leder till hög risk för enskildas fri- och rättigheter ska den personuppgiftsansvarige göra en konsekvensbedömning. Se rutin för konsekvensbedömningar.

Säkerheten vid behandlingen av personuppgifter gäller under hela tiden personuppgifterna behandlas. Det behöver därför finnas ett kontinuerligt arbete med riskanalyser och konsekvensbedömningar för att vidta åtgärder utifrån förändrade risker. Exempelvis kan nya arbetssätt, nya system eller förändringar i befintliga system och tjänster (inklusive förändringar hos leverantör och underleverantör) medföra att det krävs att nya åtgärder vidtas.

För att genomföra informationsklassning, riskanalys och i förekommande fall konsekvensbedömning som krävs i syfte att säkerställa rätt säkerhetsnivåer är ett fungerande samarbete mellan olika aktuella funktioner som arbetar med dataskydd, informationssäkerhet, it och aktuella verksamheter en nyckelfaktor.

3.2.6 Överföring till tredjeland

I dataskyddsförordningen artikel 44 regleras möjligheten att överföra personuppgifter till tredjeland (länder utanför EU/EES). Överföring kan exempelvis vara

- att personuppgifter lagras eller behandlas på annat sätt i en molntjänst som är baserad i tredjeland. Personuppgifter görs därmed tekniskt tillgängliga för

en tjänsteleverantör som kan bli skyldig att överlämna personuppgifterna till tredjeland om företaget omfattas av det landets lagar.

- att personuppgifter lagras på exempelvis en server utanför EU/EES.

- att en person som befinner sig utanför EU/EES ges elektronisk åtkomst till personuppgifter som lagras i EU/EES.

Överföring av personuppgifter till tredjeland får endast ske under vissa förutsättningar. Vissa länder har EU-kommissionen beslutat har en adekvat skyddsnivå, till dessa länder kan personuppgifter överföras på samma sätt som inom EU/EES. Utanför dessa länder kan överföring i vissa fall ske med stöd av standardavtalsklausuler som godkänts av EU-kommissionen eller genom bindande företagsbestämmelser.

Om överföring ska ske med stöd av standardavtalsklausuler eller bindande företagsbestämmelser behöver den personuppgiftsansvariga också säkerställa att den registrerade ges samma rättigheter i mottagarlandet som denne ges i ett medlemsland i EU/EES. Detta är en bedömning från fall till fall och kräver att den personuppgiftsansvariga utreder om det aktuella landets lagstiftning ger likvärdigt skydd som dataskyddförordningen.

Riskanalys och konsekvensbedömning behöver alltid göras innan nya systemavtal eller andra samarbeten ska ingås som kan innebära tredjelandsöverföring av personuppgifter.

3.2.7 Anlitande av personuppgiftsbiträde

Den som är personuppgiftsansvarig ansvarar för att det finns ett skriftligt avtal med personuppgiftsbiträdet om den behandling av personuppgifter som biträdet ska genomföra. Det kallas personuppgiftsbiträdesavtal.
Se rutin och mall för personuppgiftsbiträdesavtal på intranätet.

3.2.8 Inbyggt dataskydd (privacy by design)

Inbyggt dataskydd innebär att det tas hänsyn till integritetsskyddsreglerna redan vid utformningen av IT-system och rutiner. Det är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas.

Principen om inbyggt dataskydd bör alltid beaktas vid inköp och upphandling och under hela IT-systemets livscykel.

3.2.9 Dataskydd som standard (privacy by default)

Kravet på dataskydd som standard innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst för är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas. Principen om dataskydd som standard bör alltid tillämpas vid behandling av personuppgifter.

3.2.8 Register över personuppgiftsbehandlingar (registerförteckning)

Varje nämnd ska enligt artikel 30 i dataskyddsförordningen föra ett register över sina behandlingar av personuppgifter. Register ska upprättas skriftligen och hållas uppdaterade. Detta görs i kommunens system för registerförteckningar.

3.2.9 Gallring och arkivering

Personuppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det finns dock krav i andra författningar på att bevara uppgifter viss tid, t.ex. för redovisnings- eller arkivändamål. Genom dokumenthanteringsplan eller interna rutiner kan dessa åtgärder tydliggöras och införas i verksamheten. Det finns ingen bestämd tidsgräns för hur länge personuppgifter får behandlas, utan tidsgränsen måste bedömas från fall till fall utifrån aktuellt regelverk och ändamålet med behandlingen.

4 Organisation, ansvar och roller

Organisationen utgör arbetsstrukturen som gäller i Falköpings kommun. Syftet med organisationen är att kunna arbeta mer effektivt och strukturerat med informationssäkerhet och dataskydd inom kommunen både övergripande och på verksamhetsnivå.

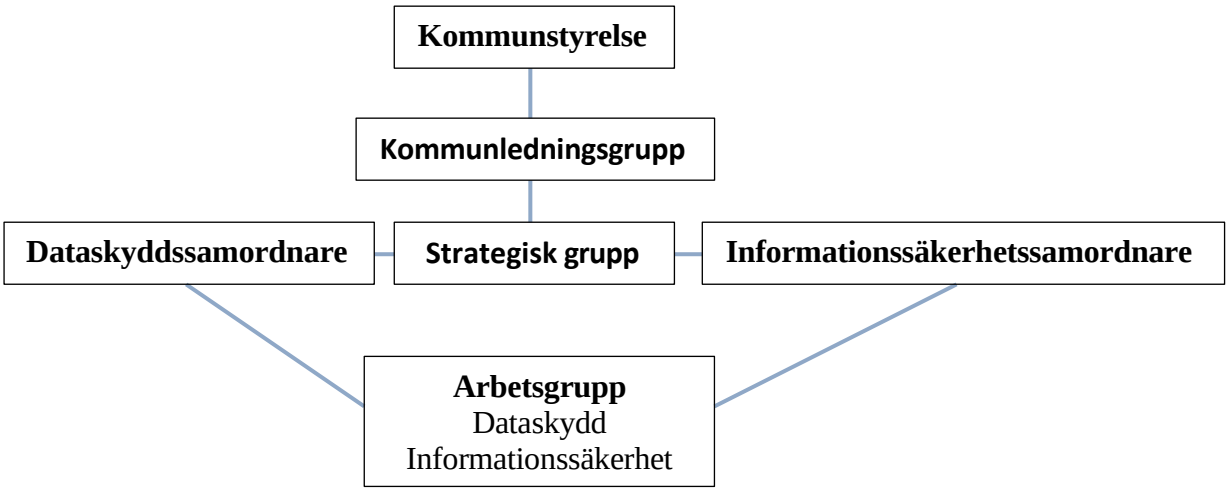
Kommunstyrelsen har ansvaret för dataskydd- och informationssäkerhetsarbetet i kommunen. Uppdraget för dataskydd har kommunledningsförvaltningen och dataskyddsamordnaren ansvarar för samordningen av det strategiska dataskyddsarbetet samt stödjer det operativa arbetet i förvaltningarna genom arbetsgruppen.

Informationssäkerhetsuppdraget finns på samhällsskyddsförvaltningen och informationssäkerhetssamordnaren ansvarar för det strategiska arbetet samt stödjer förvaltningarnas operativa arbete genom arbetsgruppen.

Strategisk grupp leder och samordnar arbetet för informationssäkerhet och dataskydd samt på en strategisk nivå med årsplanering och hur målen ska uppfyllas och följas upp. Deltagare i gruppen är informationssäkerhetssamordnare, dataskyddssamordnare, digitaliseringschef och kanslichef samt vid behov tas andra funktioner in.

Arbetsgrupp består av koordinatorer från varje förvaltning samt från det kommunala bolaget Falköpings hyresbostäder som driver det operativa arbetet inom respektive förvaltning med informationssäkerhet- och dataskydd. Informationssäkerhet- och dataskyddssamordnare leder och samordnar arbetet i gruppen. Därutöver ingår representanter från centrala funktioner i kommunen.

4.1 Organisation för informationssäkerhet och dataskydd



Figur 1: Kommunikation och förankringsmodell

Den politiska ledningen i form av kommunfullmäktige har det yttersta ansvaret för kommunens informationssäkerhet genom att ha antagit en kommunövergripande policy. Kommunstyrelsen fastställer riktlinjen som konkretiserar policyn.

Kommunstyrelsen fastställer riktlinjen för informationssäkerhet och dataskydd. I sin ledningsfunktion ingår att kommunstyrelsen ska ha uppsikt över övriga nämnders verksamhet (uppsiktsplikten). Kommunstyrelsen är arkivmyndighet och ska som sådan utöva tillsyn beträffande arkivbildning samt arkivvården i kommunen.

Respektive nämnd är ansvarig för den information som nämnden hanterar liksom och är personuppgiftsansvarig för de personuppgifter som hanteras i dess verksamhet. Nämnden ska kunna rapportera status kring sin hantering av information till kommunstyrelsen. Nämnden ska enligt 6 kap. 6 § kommunallagen (2017:725) se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten.

Kommundirektör ansvarar för att informationssäkerhetsarbetet bedrivs enligt styrdokumenten och beslutar om de övergripande rutinerna som rör informationssäkerhet och dataskydd

Förvaltningscheferna är ansvariga för informationssäkerheten inom respektive verksamhet. Förvaltningschefen ska säkerställa att förvaltningens informationssäkerhetsarbete bedrivs enligt gällande policy och riktlinjer

samt avsätta tillräckliga resurser, tid samt ge mandat till utsedd informationssäkerhetskoordinator och dataskyddskoordinator för att nå en tillräcklig nivå av informationssäkerhet och följa reglerna för dataskydd. Förvaltningschefen ska även kunna rapportera status på arbetet till berörd nämnd, kommundirektören, informationssäkerhetssamordnare och dataskyddssamordnare i Falköpings kommun. Det är förvaltningschefen ytterst som tillsätter resurser som ska läggas på informationssäkerhet inklusive dataskydd.

Digitaliseringschef ska leda och samordna informationssäkerhetsarbetet för kommunens IT-infrastruktur.

IT-säkerhetsansvarig ansvarar för att säkerheten i den interna IT-miljön, såsom tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt policyn för informationssäkerhet och dataskydd med underliggande styrdokument. IT-säkerhetsansvarig ska verka för höjande av säkerhetsmedvetande inom IT. IT-säkerhetsansvarig ansvarar även för att samordna och stödja systemägare i val av relevanta säkerhetsåtgärder och deltar vid informationsklassningar och kravställningar i upphandlingar.

Informationssäkerhetssamordnaren stödjer förvaltningarna och informationssäkerhetskoordinatorerna i det operativa arbetet med informationssäkerhet. Samordnar och leder arbetsgruppen samt deltar i den strategiska gruppen. Inom ansvarsområdet är bl.a. redovisning och uppföljning av informationssäkerhetsarbetet samt skapa och uppdatera styrdokument.

Informationssäkerhetskoordinatorn driver och stödjer förvaltningens olika funktioner i informationssäkerhetsarbetet. Exempel på stödjande funktioner är informationsklassning, riskanalyser, upphandling och incidenthantering.
Koordinatorerna deltar i kommunens arbetsgrupp för informationssäkerhet- och dataskydd. Hur mycket tid rollen som informationssäkerhetskoordinator tar varierar beroende på den aktuella förvaltningens storlek och behov.

Dataskyddssamordnare stödjer förvaltningarna och dataskyddskoordinatorerna i det operativa arbetet med dataskydd.
Den samordnande dataskyddskoordinatorn har en samordnande funktion i arbetsgruppen och ingår i den strategiska gruppen. I arbetsuppgifterna ingår bl.a. att sammankalla till arbetsgruppsmöten och ansvarar för att styrdokument tas fram och uppdateras.

Dataskyddskoordinator finns i verksamheterna och är kontaktpunkt både för registrerade och för medarbetare. Personen behöver vara insatt i de personuppgiftsbehandlingar som nämnden ansvarar för och hålla registret för behandlingarna uppdaterat, enligt artikel 30 i dataskyddsförordningen. Personen behöver delta i frågor som gäller personuppgiftsbehandlingar i verksamheten, och t ex medverka vid konsekvensbedömningar.

Dataskyddskontaktpersonen är en första kontakt vid personuppgiftsincidenter enligt gällande rutin. Hur mycket tid rollen som dataskyddskoordinator tar varierar beroende på den aktuella förvaltningens storlek och behov.

Dataskyddsombud ska utses av nämnd och har som uppgift att övervaka och rapportera om efterlevnaden av gällande dataskyddslagstiftning samt ge råd och vägledning i dataskyddsfrågor. Dataskyddsombudet är även kontaktperson för de registrerade och för tillsynsmyndigheten. Dataskyddsombudet har inget eget ansvar för att organisationen följer dataskyddsförordningen. Det ansvaret ligger alltid hos den personuppgiftsansvariga. Personuppgiftsansvarig får heller inte bestraffa dataskyddsombudet för att ha utfört sina arbetsuppgifter. Dataskyddsombudet ska alltid vara inblandat om en organisation gör, eller överväger att göra, en konsekvensbedömning för behandling av personuppgifter.

Systemägare är den person som har det övergripande ansvaret för ett IT-system. IT-systemet hanterar alltid en eller flera informationsmängder. Systemägaren ansvarar för leverans av ett system eller tjänst samt säkerställer att det finns ekonomiska och personella resurser. Systemägare tillsammans med informationsägare ställer krav på tjänsteleverantörer och driftoperatörer.

Systemförvaltare förvaltar systemet på uppdrag av systemägaren, d.v.s. inom givna ekonomiska ramar och fastställd förvaltningsplan. Systemförvaltare har det funktionella ansvaret för systemet. För större system kan en systemförvaltare ha hjälp av en IT-säkerhetsansvarig.

Informationsägare ansvarar för informationstillgångarna och är därmed riskägare. Informationsägaren ansvarar för att informationsklassning av tillgångar sker och beslutar om skyddsnivån utifrån klassningsvärdet samt ansvarar för att ställa krav på leverantör av tjänst/drift. Ett exempel från informationshantering i Microsoft 365 (MS365) på informationsägare. Varje användare är informationsägare för den egna informationen i MS 365, det vill säga egna sparade dokument, innehåll i chattar, lista över mottagare, eventuella kalenderuppgifter med mera.

Medarbetare och förtroendevalda hanterar kommunens informationstillgångar och har ett ansvar att följa kommunens policy för informationssäkerhet och dataskydd och underliggande styrdokument. De har också ansvar för att uppmärksamma fel och brister i informationshantering, utrustning och informationsinnehåll samt för att rapportera brister och incidenter i enlighet med fastställda rutiner.

3 Utbildning av medarbetare och förtroendevalda

Utbildning och kunskapsbehoven för varje målgrupp finns beskrivet i handlingsplanen som upprättas och justeras årligen.

Årlig utbildning för medarbetare och för nyanställda inom kommunen beskriv mer detaljerat i utbildningsplanen för informationssäkerhet och dataskydd.

4 Incidentrapportering

En informationssäkerhetsincident innebär en händelse som kan eller har påverkat konfidentialitet, riktighet eller tillgänglighet av information. Alla som använder information inom organisationen måste rapportera säkerhetsbrister och incidenter. Exempel på sådana händelser kan vara obehörig åtkomst till lokaler, läckage av information, försvunnen information, delade lösenord eller skadlig kod i IT-miljön. Informationssäkerhetsincidenter omfattar både tekniska och administrativa aspekter.

Informationssäkerhet- och dataskyddssamordnare ansvarar för att rutiner finns för att upptäcka, analysera och rapportera säkerhetsincidenter. Rutinerna bör inkludera rapporteringsskyldighet, rapporteringsmetod, innehåll och mottagare. Lärdomar från incidenter bör användas för att förbättra säkerheten, exempelvis genom att investera i nya lösningar eller införa nya rutiner och kontroller.

Anmälan av informationssäkerhetsincidenter följer samma process som för IT-säkerhetsincidenter. Processen omfattar mottagning, styrning, analys, återkoppling och vidarebefordran till ansvariga och berörda personer.

Vissa incidenter kräver snabb rapportering till tillsynsmyndigheter, så en bedömning av incidenten bör påbörjas omedelbart. Exempel på sådana incidenter är personuppgiftsincidenter enligt dataskyddsförordningen och incidenter som rör säkerheten i nätverk och informationssystem inom samhällsviktiga tjänster enligt NIS-direktivet.

För personuppgiftsincidenter finns särskilda rutiner och stödmaterial för att bedöma om incidenten ska rapporteras till tillsynsmyndigheten. Den utsedda dataskyddskoordinatorn inom respektive verksamhet leder arbetet med incidentrapportering och tar vid behov kontakt med olika stödfunktioner enligt rutinen.