TRANEMO KOMMUN

RIKTLINJER

Informationssäkerhet och dataskydd

Styrdokument
Handlingstyp: Riktlinjer för informationssäkerhet och dataskydd
Diarienummer: KS/2020:570
Beslutas av: Kommunstyrelsen
Fastställelsedatum: 2020-12-21 §244
Dokumentansvarig: Funktionschef medborgarservice och processtöd
Revideras: Minst vart 4:e år
Följs upp av: Kommunstyrelsen
Tidigare versioner: -
Giltig t o m: 2024-12-31

Alla beslut som rör barn ska vara barnrättsbaserade i enlighet med barnkonventionen. Beslut ska alltid föregås av prövning av barnets bästa och i större frågor samt vid beslut som kan ha negativ inverkan på barnet/barnen, ska föregås av en barnkonsekvensanalys.

Innehåll

1 Inledning

Information är värdefullt och behöver skyddas efter behov. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Detta skapar förtroende både inom och utanför organisationen.

Information är medlet för att förmedla kunskap. Information kan kommuniceras, information kan lagras, information kan förädlas och information kan styra processer – information behövs för det mesta som en kommun gör helt enkelt.

En del information är värdefull, både för organisationer och för den enskilda människan. Information är allt från forskningsresultat och fotografier till fastighetsförteckningar och saldot på bankkonto. Ibland är information livsviktig såsom informationen i patientjournaler eller styrsystemen i vattenverk. Är informationen förlorad eller felaktig kan det få katastrofala följder.

Därför måste vi skydda vår information så:

- att den alltid finns när vi behöver den (tillgänglighet)
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den och att den skyddas för obehörig insyn (konfidentialitet)

Skyddet ska anpassas efter behovet så att det är tillräckligt bra, så enkelt som möjligt att använda och är kostnadseffektivt. De konsekvenser som kan inträffa med bristande skydd är för höga för att försummas.

Brister i hantering av information leder till ett försämrat förtroende för tjänster och bakomliggande aktörer. Allvarliga och upprepade störningar kan leda till förtroendekriser, som också kan sprida sig till fler aktörer och tjänster och även till andra sektorer. Exempelvis kan ett försämrat förtroende för en kommunal verksamhet smitta av sig till andra kommunala verksamheter.

Genom god informationssäkerhet i samhället kan man främja:

- samhällets effektivitet och kvalitet i informationshantering
- näringslivets lönsamhet och tillväxt
- samhällets brottsbekämpning och beredskap mot allvarliga störningar och kriser
- medborgares fri- och rättigheter samt personliga integritet
- medborgares och verksamheters förtroende för informationshantering och IT-system

2 Syfte

Riktlinjen konkretiserar policyn för informationssäkerhet och dataskydd som antagits av kommunfullmäktige. Riktlinjen ger tydliga ramar för hur kommunens informationssäkerhets- och dataskyddsarbete ska bedrivas och organiseras i förvaltningen. Kommunstyrelsen beslutar om riktlinjerna medan tillämpningar av riktlinjerna utformas i guider av informationsägare.

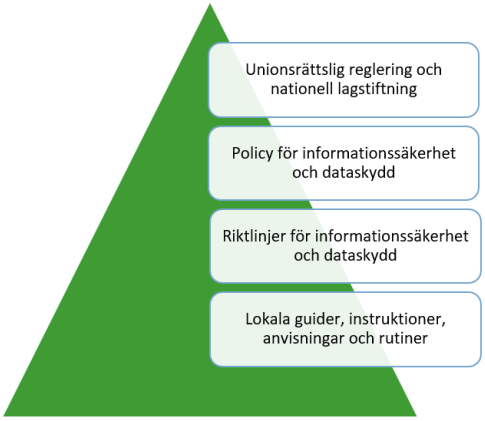

Bild: Pyramid som illustrerar hierarkin för styr- och stöddokument

3 Informationstillgångar

Med informationstillgångar avses all information och relaterade resurser/tillgångar som behövs för att hantera informationen. Exempel på resurser som används för att hantera information är IT-system, IT infrastruktur, pärmar och papper. Oavsett om informationen behandlas manuellt eller automatiserat och oberoende av dess form eller miljö den förekommer i så ska informationstillgångarna ha rätt skydd. Perspektivet med informationssäkerhet och dataskydd är en naturlig del vid utformning av våra arbetssätt och en del av vårt dagliga arbete.

Invånarna förväntar sig i allt högre grad att snabbt, enkelt och säkert kunna sköta sina ärenden, få tillgång till information och ha möjlighet till inflytande genom digitala kontaktvägar. Att information är korrekt som kommunen hanterar i relationer med kommuninvånare, företag och organisationer såväl som inom vår egen organisation utgör en grund för tillit och förtroende. Det är även viktigt att information i alla externa och interna relationer är tillgänglig när det behövs och att känslig information skyddas för att vi ska kunna fullgöra vårt uppdrag i samhället. Informationens säkerhet är därför en mycket viktig aspekt för alla verksamheter (informationsägare) inom kommunen. Informationssäkerhets- och dataskyddsarbetet är en del i kommunens lednings- och kvalitetsarbete och omfattar alla informationstillgångar och personuppgifter utan undantag. Implementering och tillämpning

3.1 Informationssäkerhet

Arbetet med informationssäkerhet omfattar att införa och förvalta **administrativa regelverk** som policys och riktlinjer, **tekniskt skydd** med bland annat brandväggar och

kryptering samt **fysiskt skydd** med till exempel skal- och brandskydd. Det handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver.

Informationssäkerhet är teknikneutralt och omfattar skydd av såväl muntlig, pappersbunden som digital information. Utgångspunkten för kommunens informationssäkerhetsarbete är att följa den etablerade standarden inom området, SS-ISO/IEC 27000, Dataskyddsförordningen (GDPR) och övriga tillämpliga lagar inom dataskydd. Detta stämmer väl överens med Myndigheten för samhällsskydd och beredskaps (MSB) rekommendation om hur informationssäkerhetsarbetet ska bedrivas inom offentlig förvaltning.

3.2 Dataskydd

Dataskydd handlar om att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Dataskyddsförordningen (The General Data Protection Regulation, GDPR) gäller i hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras. Vidare finns den nationella regleringen, SFS lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, även benämnd som dataskyddslagen. Dataskydd finns även reglerat i flera andra lagstiftningar som alltid ska beaktas i verksamheternas arbete.

3.3 LISD

För att kunna arbeta strukturerat med informationssäkerhet och dataskydd införs ett ledningssystem för informationssäkerhet och dataskydd, LISD. Systemet bygger på SS-ISO/IEC 27000. För implementering och tillämpning utgår kommunens arbete från stöd på www.informationssakerhet.se som tagits fram av myndigheten MSB i samverkan med andra myndigheter. Som komplement används även Västra Götalandsregionens verktygslåda för informationssäkerhet.

3.4 Informationsklassning

Grunden för att kunna ge informationstillgångar rätt skydd är att inventera, värdera och klassificera informationstillgångarna.

Kommunens samtliga informationstillgångar ska finnas förtecknade i kommunens informationshanteringsplan (IHP), därmed utgör IHP en grund för värdering och klassificering av informationen utifrån informationssäkerhet och dataskydd.

För att underlätta informationshanteringen med externa aktörer utgår kommunens klassningsmodell från myndigheten MSB:s klassningsmatris med anpassning av definitioner av konsekvens- och skyddsnivåer utifrån kommunens förutsättningar. Varje informationstillgång värderas sedan inom varje säkerhetsaspekt tillgänglighet, riktighet och konfidentialitet.

Genom att klassa informationstillgångar utifrån de tre säkerhetsaspekterna identifieras vilken effekt otillräckligt skydd av informationstillgångarna får och utifrån det säkerställs att kraven på informationssäkerhet och dataskydd är på rätt nivå. En viss information kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet. Klassning syftar främst till att ge tillräckligt skydd för kritiska informationstillgångar, men också till att undvika överskydd med onödigt höga kostnader som följd.

Klassningsmodellens roll är att skapa en organisationsgemensam ram så att klassning sker på ett enhetligt sätt i hela organisationen och att samma skyddsnivå ges till likvärdiga informationstillgångar.

Själva informationen är den primära tillgången som klassas, resurser som används för att hantera informationen ska sedan utformas så att de möter de krav som klassningen av informationen medför enligt de skyddsåtgärder som klassningsmodell beskriver.

För att kunna bedöma att informationstillgångar har rätt skydd ska SKR:s (Sveriges kommuner och regioner) klassningsverktyg KLASSA användas för att göra självskattning och ta fram åtgärdsplan.

4 Delmål

För att nå de strategiska målen i policyn för informationssäkerhet och dataskydd har ett antal delmål inom olika områden identifierats.

Område	*Delmål*
Organisation	Organisationen ska ha ett högt riskmedvetande och informationssäkerhetsarbetet ska vara organiserat så att det finns tydligt mandat och ansvar.
Riskhantering	Risker som kan påverka kommunens informationssäkerhet ska identifieras, analyseras och hanteras.
Styrning av informationstillgångar	Alla informationstillgångar ska vara kopplade till en informationsägare som har ansvar för att informationen och resurserna klassificeras och skyddas på rätt sätt.
Åtkomst till information	Användare ska ha tillgång till rätt information på rätt sätt för sin arbetsuppgift och vara medveten om sitt personliga ansvar.
Personal och säkerhet	Alla medarbetare som hanterar informationstillgångar ska ha kännedom om kommunens styrdokument och regelverk och tillräcklig kompetens för att kunna utföra sina arbetsuppgifter på ett säkert sätt.
Fysisk säkerhet	Kommunens information, samt övriga informationstillgångar, som exempelvis lokaler och den utrustning som används för informationshantering, ska skyddas på en tillräcklig nivå.
Drift och kommunikation	Drift och kommunikation av IT-miljö, system och tillhörande resurser ska ske utifrån fastställda rutiner för gemensam infrastruktur och de specifika säkerhetskrav som ställs av verksamheten.
Dataskydd	Organisationen ska ha ett systematiskt arbete gällande dataskydd för att uppnå ett högt personligt integritetsskydd för anställda och innevånare.
Hantering av incidenter	En process för rapportering när det gäller informationssäkerhets- och personuppgiftsincidenter ska finnas. Detta för att mildra effekter, förhindra upprepande och underlätta återgång till verksamhet på normal nivå då någon form av incident skett.
Kontinuitetsplanering	Det ska finnas en kontinuitetsplanering för att säkerställa den tillgång till information och funktioner som krävs för att upprätthålla verksamhet.
Uppföljning	Informationssäkerheten ska, som en del av den ordinarie verksamhetsredovisningen, regelbundet följas upp på central nivå och inom respektive nämnd, styrelse och bolag.

5 Principer och arbetssätt

Arbetet med informationssäkerhet och dataskydd ska vara normerande, stödjande och kontrollerande. Arbetet ska bedrivas riskbaserat vilket innebär att hot, risker och sårbarheter identifieras och reduceras.

Principer för arbetet med informationssäkerhet och dataskydd:

- bygger på en helhetssyn som har informationen som utgångspunkt men även omfattar organisation, arbetssätt, processer, människor och teknik
- är systematiskt och bygger på den vedertagna standardserien ISO/IEC 27000 samt på rekommendationer från MSB
- aktiv samverkan med det förvaltningsarbete som finns i kommunen och där det är möjligt använda samma dokumentationsmodell
- integreras i arbetet med upphandling och avtalsuppföljning
- uttrycks i relevanta och uppdaterade styrdokument
- är förebyggande men ska även kunna hantera incidenter, allvarliga störningar och kriser när det gäller såväl säkerhets- som personuppgiftsincidenter
- förbättras och anpassas löpande i en föränderlig omvärld
- är väl kommunicerat i verksamheterna där medarbetare genom utbildning och information får en säkerhetsmedvetenhet med syfte att leva upp till denna policy och tillhörande styrdokument

6 Roller, ansvar och befogenheter

Ansvaret för kommunfullmäktige, kommunstyrelsen, nämnder med förvaltning och kommunala bolag fastslås i informationssäkerhets- och dataskyddpolicyn. För att kunna upprätta ett gott informations- och dataskydd krävs ytterligare utpekade roller, ansvar och befogenheter inom kommunen.

Kommunchef ansvarar på uppdrag av kommunstyrelsen för att informationssäkerhets- och dataskyddsarbetet bedrivs så effektivt som möjligt så att informationssäkerhet och dataskydd uppnås enligt kommunstyrelsen och kommunfullmäktiges beslut.

Chef/VD ansvarar för informationssäkerhets- och dataskyddsarbetet inom sin verksamhet. Chef/VD ansvarar för att medarbetare inom den egna verksamheten har tillräcklig kunskap och förståelse för att erforderlig informationssäkerhet och dataskydd i verksamheten ska uppnås.

Informationsägare är tillika verksamhetsansvarig. Denne ansvarar för att värdera informationen och därigenom skydda information med relevanta säkerhetsåtgärder.

Informationsägaren ska planera, genomföra och återrapportera informationssäkerhetsarbetet.

Medarbetare är ansvariga för att följa kommunens styrdokument (policy, riktlinjer och guider) för informationssäkerhet och dataskydd. Medarbetare har också ansvar att uppmärksamma brister och incidenter rörande informationssäkerhet och dataskydd och rapportera dessa till närmaste chef.

Dataskyddsombud (DSO) utses av varje nämnd och bolagsstyrelse. Dataskyddsombuden bevakar att personuppgiftsansvarig lever upp till dataskyddsförordningen och annan relevant lagstiftning. Detta görs genom rådgivning, utbildning och vägledning samt genom olika former av granskningar.

Säkerhetssamordnaren i kommunen arbetar strategiskt med krisberedskap och civilt försvar. Informationssäkerhet är en del av totalförsvaret och det civila försvaret där bland annat kommunerna har en viktig roll. Säkerhetssamordnaren sitter med i Informationssäkerhetsgruppen (ISG).

Informationssäkerhetssamordnaren (CISO) har i uppdrag att utveckla, leda, samordna och granska informationssäkerhetsarbetet inom kommunen. Detta innefattar kontinuerlig revidering av ledningssystemet för informationssäkerhet och dataskydd (LISD) och regelbunden rapportering till kommunstyrelsen och kommunchef kring informationssäkerhets- och dataskyddsarbetet.

Dataskyddskontakt (DSK) är den funktion som är kontaktperson gentemot dataskyddsombud och jobbar strategiskt och operativt med dataskydd i kommunen. Dataskyddskontakten sitter med i ISG.

Informationssäkerhetsgruppen (ISG) samordnar och följer upp informationssäkerhets- och dataskyddsarbetet. Informationssäkerhetssamordnaren är sammankallande och leder arbetet i ISG. Informationssäkerhetssamordnaren har mandat att utifrån aktuella ämnen kalla in andra deltagare till gruppen. Gruppen ska sammanträda regelbundet och rapportera om sin verksamhet till IT-styrgruppen.

Informationssäkerhetshandläggare utses för varje sektion eller motsvarande. Funktionen ska arbeta aktivt med informationssäkerhet och dataskydd inom sin verksamhet och ingår i kommunens informationssäkerhetsnätverk.

Nätverk för informationssäkerhet består av ISG och informationssäkerhetshandläggare. Nätverket sammankallas av Informationssäkerhetssamordnaren. Nätverket träffas regelbundet för gemensamt arbete, erfarenhetsutbyte och kunskapshöjande insatser inom området.

IT-chef ansvarar för kommunens interna tekniska IT-miljö och säkerställer att IT-miljön är tillförlitlig och motsvarar interna och externa krav gällande informationssäkerhet och dataskydd. Har ett övergripande ansvar för att säkerställa ett grundskydd för information hanterad i IT-verksamheten.

IT-säkerhetsansvarig ansvarar för att säkerheten i den interna IT-miljön, såsom tjänster, processer, system, infrastruktur, verktyg etcetera är tillräcklig och uppfyller verksamheters krav, legala krav samt policyn för informationssäkerhet och dataskydd med underliggande styrdokument. Verka för höjande av säkerhetsmedvetande inom IT. Ansvarar för att samordna och stödja informationsägare i val av relevanta säkerhetsåtgärder och deltar vid informationsklassningar och kravställande i upphandlingar. IT-säkerhetsansvarig sitter med i ISG.

IT-styrgruppens sammansättning och uppdrag regleras av IT-samverkan, kommunchefer från samverkande kommuner sitter med i IT-styrgruppen. Säkerhetssamordnaren ingår i IT-styrgruppen och rapporterar fortlöpande arbetet kring informationssäkerhet- och dataskyddsarbetet samt lyfter behov av gemensamma beslut till IT-styrgruppen.