Fastställd: Kommunstyrelsen 2022-06-14, § 139

Gäller för: Samtliga nämnder
Dokumentansvarig:
Informationssäkerhetssamordnare

Dnr : **KS2022/63-9**

Riktlinjer för informationssäkerhet och dataskydd

Innehållsförteckning

1. Inledning

Information är värdefullt och fordrar att man skyddar efter behov. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Detta skapar förtroende både inom vår organisation och för kommunens medborgare.

Information är verktyget för att förmedla kunskap. Vi kan kommunicera information, vi kan lagra den, vi kan förädla den och vi kan styra processer med den. Vi behöver den för det mesta vi gör helt enkelt.

I vår **Policy för informationssäkerhet och dataskydd** KF 2022-05-05 §49 står det att, ”Syftet med denna policy är att säkerställa att rätt och riktig information ska nå rätt mottagare i rätt tid och vara skyddad för obehörig åtkomst och förstörelse”. Därför måste vi skydda informationen som vi hanterar utifrån tre säkerhetsaspekter. Dessa aspekter är, konfidentialitet, riktighet och tillgänglighet.

Det innebär att vi skyddar informationen så att:

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

Skydd ska anpassas efter våra behov och vara så bra som verksamheten kräver, 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 vår hantering av information leder till ett försämrat förtroende för de tjänster kommunen ansvarar för och våra personuppgiftsbiträden. Allvarliga och upprepade störningar kan leda till förtroendekriser, som också kan sprida sig till andra förvaltningar i kommunen. Ett försämrat förtroende för en förvaltning kan smitta av sig till andra delar av kommunens verksamheter.

2. Syfte

Syftet med denna riktlinje är att konkretisera **Policyn för informationssäkerhet och dataskydd**, som antagits av kommunfullmäktige. Riktlinjen ger tydliga ramar för hur kommunens informationssäkerhets- och dataskyddsarbete ska bedrivas och organiseras i Bollebygd kommun.

Kommunstyrelsens beslut av riktlinjer för informationssäkerhet och dataskydd betyder att informationsägarna i varje förvaltning utformar egna rutiner och anvisningar för detta arbete.

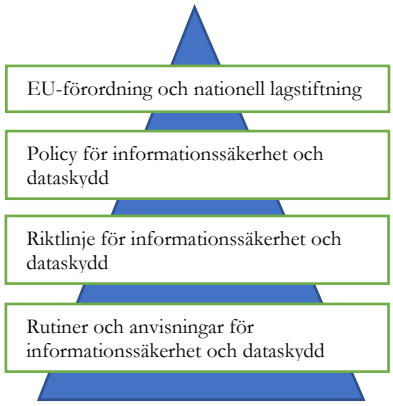

Bild 1: Ordningen för styr- och stöddokument för detta arbete visas i bilden ovan.

3. Informationstillgångar

Med informationstillgångar menas all information, resurser och 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.

Kommunens invånare 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 förhållanden 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 inom kommunen. Informationssäkerhets- och dataskyddsarbetet är en del i kommunens lednings- och kvalitetsarbete och omfattar alla informationstillgångar och personuppgifter utan undantag.

3.1 Informationssäkerhet

Arbetet med informationssäkerhet består av 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 de upprättade standarderna inom området, SS-ISO/IEC 27000-serien, Dataskyddsförordningen (GDPR) och övriga lagar inom dataskydd. Detta överensstämmer med Myndigheten för samhällsskydd och beredskaps (MSB) och Informationssäkerhet.se 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 (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 27000–27002. 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

Klassning av informationstillgångarna är en förutsättning för att skapa rätt skydd för informationen och undvika överskydd med höga kostnader och krångliga rutiner som följd. Klassning ska ske på ett enhetligt sätt i hela organisationen så att likvärdig information får samma skyddsnivå.

Samtliga informationstillgångar ska finnas listade i kommunens registerförteckning, därmed utgör registerförteckningen 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, (se ovan) 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 gemensam 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. Målsättning

För att kunna åstadkomma de strategiska målsättningarna i policyn för informationssäkerhet och dataskydd har ett antal målsättningar inom olika områden identifierats.

Område	Delmål
Organisation	Förvaltningarna 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 informationstillgångarna	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 informations-säkerhets- 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.