Informationssäkerhetspolicy

Antagen av kommunfullmäktige den 22 februari 2024

Dokumenttyp: Policy
Diarienummer: KS 2023/65
Giltighetstid: Tills vidare
Dokumentansvarig: Kanslichef

Ragunda Kommun

Innehållsförteckning

1 Syfte, mål, omfattning och uppföljning

1.1 Syfte

Informationssäkerhetspolicyn pekar ut omfattningen och inriktning för informationssäkerhetsarbetet i Ragunda kommun.

1.2 Mål

Informationssäkerhetspolicyns mål är att säkerställa att förutsättningar ges för att både ett systematiskt riskbaserat och långsiktigt informationssäkerhetsarbete utvecklas och upprätthålls i Ragunda kommun. Detta för att skydda kommunens skyddsvärda information, dess invånare och vårdtagare samt kommunens medarbetare och dess verksamhet, som annars riskerar att skadas genom bristande informationssäkerhet.

1.3 Omfattning

Informationssäkerhetspolicyn gäller för alla verksamheter inom Ragunda kommun. Samtliga anställda, såväl politiker som tjänstemän och extern personal (exempelvis konsulter och praktikanter etc.) omfattas av alla dokument rörande informationssäkerhet.

1.4 Uppföljning

Kommunens Informationssäkerhetssamordnare, ansvarar för att uppföljning och revidering av informationssäkerhetspolicyn utförs minst en gång varje år om behov av detta identifierats. I samband med revidering ska samtliga styrdokument inom informationssäkerhet ses över och vid behov uppdateras.

Kommunledningen ska minst en gång per år informera sig om hur arbetet med kommunens informationssäkerhet går. Genomgången görs vid den årliga aktiviteten ”ledningens genomgång”. Uppföljningen ska baseras på underlag med rekommendationer som tas fram av Informationssäkerhetssamordnare. Underlaget bör vara behovsstyrt men kan innefatta information om:

Förändringar utanför kommunen som kan påverka informationssäkerheten

- Utbildning (status och behov)
- Inträffade incidenter av större påverkan på verksamheten.
- Resultat från eventuellt genomförda granskningar
- Aktuella och planerade säkerhetsåtgärder
- Rekommendationer till åtgärder och förbättringar

2 Informationssäkerhet

2.1. Om information och informationssäkerhet

Information är medlet för att förmedla kunskap och budskap. Information kan kommuniceras, lagras, förädlas och användas för att styra processer samt fatta beslut, information är således en av Ragunda kommuns viktigaste tillgångar. Arbetet med att skydda informationen, officiellt kallat: Informationssäkerhet, är en viktig del för att kommunens verksamheter ska fungera.

För att informationen ska kunna skyddas inom Ragunda kommun måste skyddsvärd information identifieras, därför måste informationssäkerhetsarbetet vara en integrerad del i alla av kommunens verksamheter, ytterligare måste arbetet ständigt utvecklas och anpassas efter aktuella sårbarheter samt risk- och hotbilder, både vad avser yttre såväl som inre hot.

2.2. Definition av informationssäkerhet

Informationssäkerhet handlar om bevarandet av konfidentialitet, riktighet och tillgänglighet hos kommunens skyddsvärda information, detta genom att skapa och upprätthålla korrekta samt lämpliga skydd av kommunen information under hela dess livstid, detta innebär att information som identifierats som skyddsvärd ska skyddas från dess att den skapas till att informationen förstörs.

Informationssäkerhet innefattar all information i verksamheten utan undantag, oavsett om den är öppen eller hemlig samt om den behandlas manuellt eller automatiserat- och oberoende av vilken form eller miljö den lagras, kommuniceras eller bearbetas inom. Information kan vara materiell exempelvis papper, hårddiskar eller text på en whiteboardtavla, information kan också vara immateriell, exempelvis konversationer mellan personer och kunskap som enskilda individer besitter. Det är ägaren av informationstillgången som bedömer om den är skyddsvärd eller inte. Hur skyddsvärt något är beror på vilken konsekvens det får om exempelvis informationstillgången hamnar i fel händer eller inte är nåbar.

Konsekvenserna av bristande informationssäkerhet kan bli allvarliga, exempelvis att informationstillgångar röjs för obehöriga, att information görs otillgänglig eller manipuleras. Ett exempel på allvarliga konsekvenser är om sjukvårdsjournaler inte går att läsa eller inte går att lita på.

Informationstillgångar som är skyddsvärd måste skyddas på ett korrekt och lämpligt sätt mot de sårbarheter, risker och hot som förekommer både internt och externt.

Informationssäkerhetsarbetet inom Ragunda kommun utgår från tre aspekter:

- **Tillgänglighet**: Information ska kunna användas i förväntad utsträckning och inom önskad tid. Detta oavsett om det gäller en kort eller lång tidsaspekt.
- **Riktighet**: Information ska varken kunna ändras eller bli manipulerad av misstag.
- **Konfidentialitet**: Information får inte röjas vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.

3 Ragunda kommuns förhållningssätt rörande informationssäkerhet

Informationssäkerhet består av organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder. Den organisatoriska säkerheten består bland annat av styrning, roller, ansvar, regelverk och processer. Personrelaterade åtgärdar handlar mycket om medvetenhet och utbildning. Fysiska åtgärder innefattar skalskydd, skydd mot fysiska och miljörelaterade hot, arbete i säkra utrymmen och tillträde. Den tekniska säkerheten är den delen som generellt beskrivs som IT-säkerhet och ibland även cybersäkerhet. Här återfinns arbete med säkerhetsåtgärder inom nätverk, servrar, arbetsstationer samt hård- och mjukvara.

Säkerhetsåtgärder är åtgärder som vidtas för att skydda informationstillgångarna. Dessa säkerhetsåtgärder anpassas efter informationens identifierade skyddsvärden.

Ragunda kommun ska aktivt arbeta med informationssäkerhet för att identifiera interna samt externa sårbarheter, risker och hot rörande kommunens skyddsvärda informationstillgångar. Detta för att kunna skapa och upprätthålla korrekt och lämpliga skyddsåtgärder som reducerar identifierade sårbarheter, risker och hot till en av verksamheten acceptabel nivå.

3.1 Strategiska mål med informationssäkerhet

Kommunen bedriver ett långsiktigt riskbaserat och systematiskt informationssäkerhetsarbete, detta via ett Ledningssystem för informationssäkerhet (LIS), vilket bygger på den etablerade standarden för informationssäkerhet, SS-ISO/IEC 27000-serien.

3.2 Målsättning

- Kommunens informationstillgångar ska skyddas på lämplig nivå, genom identifiering av skyddsvärd information och informationsklassificering samt genomförande av risk-, hot och sårbarhetsanalyser.

- Kommunens organisation ska inneha tydlig fördelning av ansvar för informationstillgångar och med relevanta roller för ledning och genomförande av ett långsiktigt systematiskt informationssäkerhetsarbete.
- Informationssäkerhetsarbete ska vara en integrerad del av kommunens kontinuitets-, kris- och totalförsvarsarbete, i syfte att säkerställa förmågan att informationssäkerheten ska kunna upprätthållas och utvecklas oavsett om det råder fred, kris, eller krig.
- Chefer, medarbetare, förtroendevalda och inhyrd personal ska ha tillräckligt med kunskaper och utbildning inom informationssäkerhet för att kunna bidra till en god säkerhetskultur och att skyddet av kommunens informationstillgångar upprätthålls och utvecklas.
- Informationssäkerhet ska vara en integrerad del av varje verksamhet där risk-, hot och sårbarhetsanalyser samt informationsklassificeringar sker kontinuerligt.
- Informationssäkerhet ska beaktas under informationstillgångens hela livscykel, från upprättande till införande och arkivering samt förstörelse.

4 Ansvar inom informationssäkerhetsarbetet

Ansvaret för informationssäkerhetsarbetet följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens Informationssäkerhetssamordnare ansvarar för att stödja verksamheterna i att uppnå för verksamheten en acceptabel nivå av informationssäkerhet.

4.1 Den politiska ledningen

Kommunfullmäktige, kommunstyrelse, nämnder och bolagsstyrelser har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom deras ansvarsområden.

4.2 Informationsägare

All information ska ha en utsedd/fastställd informationsägare. Informationsägaren ansvarar för informationssäkerheten inom sin egen verksamhet. Detta innebär att informationsägaren kontinuerligt identifierar skyddsvärda informationstillgångar, genomför lämpliga risk-, hot- och sårbarhetsanalyser samt klassificerar informationen och framarbetar skyddsåtgärder. Informationsägaren ansvarar också för att skyddsåtgärderna implementeras och vidmakthålls i verksamheten.

4.3 Medarbetare och förtroendevalda

Medarbetare och förtroendevalda ansvarar för att följa informationssäkerhetspolicyn och andra anknutna styrdokument. Varje medarbetare och förtroendevald som hanterar informationstillgångar i någon form har också ansvar för att upprätthålla informationssäkerheten och förbinder sig att följa de säkerhetsföreskrifter som finns beslutade. Enskilda medarbetare och förtroendevalda ansvarar således även för att vara uppmärksam på brister och incidenter rörande informationssäkerheten som sedan rapporteras via fastställda incidenthanteringsprocesser.

4.4 Informationssäkerhetssamordnare

Informationssäkerhetssamordnare har det strategiska övergripande ansvaret att stödja verksamheterna samt leda och samordna informationssäkerhetsarbetet inom kommunen. Detta arbete kan exempelvis innebära att utbilda verksamheterna inom informationssäkerhet, verka som en rådgivande funktion åt verksamheterna samt stötta verksamheterna i att identifiera skyddsvärda informationstillgångar, detta kan innebär att vara behjälplig i att identifiera risker, sårbarheter och hot mot verksamheternas skyddsvärda informationstillgångar. Informationssäkerhetssamordnaren kan också hjälpa till att genomföra informationsklassificeringar samt identifiera skyddsåtgärder.
Informationssäkerhetssamordnaren ska kontinuerligt ges möjlighet att utvecklas i sin arbetsroll samt orientera sig själv rörande händelser, risker, hot och sårbarheter som är relevanta för informationssäkerhetsarbetet.
Informationssäkerhetssamordnaren ska även ha ett nära samarbete med relevanta interna samt externa aktörer.