

Informationssäkerhetspolicy

Antagen av kommunfullmäktige: 2020-06-22

Ansvarig förvaltning: Kommunledningskontoret

Ansvarig tjänsteman: Informationssäkerhetssamordnare (Ciso)



Innehåll

Innehåll	2
Förord.....	4
Färdriktning för Vaggeryds kommuns arbete gällande informationssäkerhet	5
Bakgrund till denna informationssäkerhetspolicy	5
Principer och styrning för informationssäkerhetsarbetet.....	6
Helhetssyn.....	6
Standardisering och systematisering	7
Samverkan.....	7
Riskmedvetenhet.....	8
Regelverk	8
Ansvar	9
Grundprincip kring ansvar	9
Övergripande ansvar	9
Ansvar inom respektive verksamhet	10
Medarbetares ansvar	10

Dokument namn	Informationssäkerhetspolicy	Dokumentet gäller för	Förtroendevalda & medarbetare
Dokumentansvarig	CISO Annika Lagerqvist	Dokumentet beslutas av	Kommunfullmäktige
version	1	Giltighetstid	202006 22 -2022
Senast reviderad		Verksamhetskod/ inf. klass	2.1.1.0 K1



Informationssäkerhet är den del i organisationens lednings-och kvalitetsprocess som avser hantering av verksamhetens information.

Informationssäkerhet är en stödande verksamhet för att öka kvaliteten hos kommunens funktioner.

Policyn redovisar ledningens viljeinriktning för arbetet med informationssäkerhet.

Förord

Information uttrycker kunskap och är en tillgång för individer och organisationer. Vi kan kommunicera information, vi kan lagra den, vi kan styra processer med den – vi behöver den för det mesta vi gör helt enkelt.

Syftet med denna policy är att ange långsiktiga målsättningar, färdriktningar och arbetssätt för informationssäkerhet i Vaggeryds kommun. Informationssäkerhet handlar om hur Vaggeryds kommun förhåller sig till den information vi hanterar oavsett om den är digital eller analog. Information är en av Vaggeryds kommuns viktigaste tillgångar. Oavsett form och kanal har den en avgörande roll för kommunens verksamheter varje dag, året runt. Informationssäkerhet berör med andra ord alla. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljö den förekommer i utan undantag. Informationssäkerhet handlar därmed om mer än att säkra informationssystem. Även andra resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhetsbegreppet.

Informationssäkerhet handlar om att information ska skyddas utifrån krav på dess:

Konfidentialitet

att informationen inte tillgängliggörs eller avslöjas till obehöriga

Riktighet

att information inte kan förändras av obehöriga, av misstag eller på grund av störningar i funktion/system. Informationen ska vara korrekt, tillförlitlig och fullständig

Tillgänglighet

att informationen är åtkomlig och användbar för behöriga

Spårbarhet

att händelser i informationsbehandlingen ska kunna spåras till ett identifierat objekt ex. handling, användare, dator, skrivare eller system/program.

Färdriktning för Vaggeryds kommuns arbete gällande informationssäkerhet

Denna policy för informationssäkerhet i Vaggeryds kommun anger tillsammans med den nationella strategin och handlingsplanen för informations- och cybersäkerhet, färdriktningen för Vaggeryds kommun.

Policyn innehåller principer för informationssäkerhetsarbete som har en stor betydelse för att kommunfullmäktiges övergripande mål samt kommunens vision ska uppfyllas.

Målet för Vaggeryds kommuns arbete med informationssäkerhet är att minska sannolikheten för, eller konsekvenserna av, uppkomna eller identifierade hot mot den information kommunen har en skyldighet att skydda. Dessutom främjas invånarens rättigheter och personliga integritet samt kommunens förmåga att förebygga och hantera alvarliga störningar och kriser.

Skyddet ska vara anpassat till informationens skyddsvärde, risk och lagkrav och därmed också verka för att bevara förtroendet för kommunens verksamhet, informationshantering och övrigt IT relaterat arbete. Arbetet är långsiktigt, ska bedrivas kontinuerligt med fastställd metodik där utgångspunkten är riskhantering och tyngdpunkten ligger på förebyggande aktiviteter.

Bakgrund till denna informationssäkerhetspolicy

Policyn fastställs av kommunfullmäktige och gäller för all verksamhet inom kommunen. Detta betyder att det inte finns utrymme att besluta om lokala regler som avviker från detta. Styrdokumentet har tagits fram utifrån Myndigheten för samhällsskydd och beredskap (MSB) rekommendationer. Dessa grundar sig i sin tur på internationell standard för informationssäkerhet ISO27000- serien. Den nationella strategin för informations- och cybersäkerhet samt det it-politiska målen i digitaliseringsstrategin är bakomliggande styrdokument för policyn. Det som sägs i är av övergripande karaktär. I riktlinjer för informationssäkerhet kommer instruktioner för informationssäkerhetsarbetet att visa hur denna policy ska tillämpas.

Principer och styrning för informationssäkerhetsarbetet

Arbetet med informationssäkerhet ska gentemot Vaggeryds kommuns verksamheter vara normerande, stödjande och kontrollerande för att fastställa nödvändig kvalitetsnivå. Informationssäkerhetsarbetet ska bygga på följande principer.

Principer för informationssäkerhet

Helhetssyn

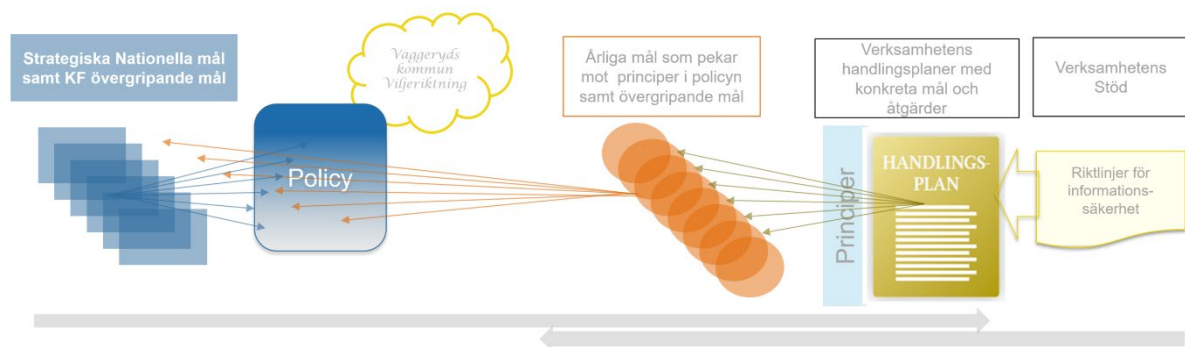
Standardisering och systematisering

Samverkan

Riskmedvetenhet

Regelverk

Ansvar



Bildbeskrivning: styrning av informationssäkerhetsarbetet

Helhetssyn

För att Vaggeryds kommun ska kunna utvecklas på ett tryggt och säkert sätt krävs att alla aktörer har en helhetssyn på informationssäkerhet.

Informationssäkerhet ska vara en självklar och integrerad del i all utveckling inom och mellan organisationer samt inom och mellan kommunens samarbetspartners. Digitalisering, IT- och informationsrelaterat arbete ökar och en säker hantering av information påverkar alla nivåer i kommunen. Säkerhetsåtgärder ska både syfta till att skapa en mer robust informationshantering vid kommunens normaltillstånd men också ge förutsättningar att hantera mer allvarliga störningar och kriser.

Standardisering och systematisering

Kommunens informationssäkerhetsarbete ska bedrivas i enlighet med ISO standarden ISO/IEC 27000, med målet att skapa ett ledningssystem för informationssäkerhet (LIS).

Genom följsamhet till standard kan en högre säkerhet uppnås och onödiga misstag undvikas. Standardisering förenklar utbildning och förbättrar även kompetenser. Standarder ökar också transparensen mellan organisationer vilket gör det lättare att ställa krav och bedöma informationsobjekt som produkter, system och hela verksamheter.

Systematiken innebär kontinuerliga uppföljningar med reviderade handlingsplaner enligt metodik: planera, genomföra, följa upp och åtgärda. För att säkerställa kvalitet och objektivitet sker granskning enligt fastställd regelbundenhet.

Samverkan

Informationssäkerhetens komplexitet, gränsöverskridande karaktär kräver en effektiv samverkan nationellt, regional och kommunalt. Kommunen ska genom samverkan stödja förebyggande åtgärder och arbeta med att främja ett systematiskt långsiktigt arbete med informationssäkerhet på alla nivåer i samhället.

På regional nivå ska kommunen samverka med Länsstyrelsen som har ett samordningsuppdrag mot Regionen och länets kommuner. Kommunen ska vara representerad i regionens informationssäkerhetsarbete. Kommunen ska också tillse att en samverkan finns mellan kommunala styrelser och nämnder

Riskmedvetenhet

Det krävs resurser för att kunna nå en säker och trygg informationshantering i samhället. Kommunen ska arbeta för ett ökat säkerhetsmedvetande i samhället och inom den egna organisationen.

Genom riskhantering, tillse samordnade aktiviteter för att styra och leda kommunen med avseende på risk. I kommunens kontinuitetsplanering ska det finnas beredskap för avbrott och störningar. Våra kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av incidenter. Detta ska övas regelbundet genom olika simulerade informationssäkerhetsincidenter.

Säkerhetsaspekter ska inte ses som en ytterligare kostnadspost, utan som en självklar investering för att uppnå avsedd funktion och kvalitet. Investeringar för att bygga in och förbättra säkerhet bör alltid jämföras med vad det kan kosta att inte göra detta. Skyddet ska vara anpassat till informationens skyddsvärde, risk och lagkrav och därmed också verka för att bevara förtroendet och tilliten till kommunens verksamhet, informationshantering och övrigt IT relaterat arbete.

Målet är att hitta rätt säkerhetsnivåer och att de ansvariga är medvetna om vilka risker som finns, för att aktivt kunna besluta om att eliminera, reducera eller acceptera dessa risker. En sådan riskmedvetenhet utgör grunden för effektiva informationssäkerhetsinvesteringar. Skyddsåtgärder ska vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en otillräcklig säkerhet kan medföra. Investeringar i informationshantering görs inte sällan i syfte att effektivisera och rationalisera tjänster i samhället. Det är därför rimligt att man satsar en del av besparingarna på att uppnå kvalitet och robusthet genom ökade säkerhetsinsatser

Regelverk

En förutsättning för en god informationssäkerhet i samhället är att det finns regler som ligger i linje med modern informationshantering. Detta gäller för både verksamhetsnivå och samhällsnivå. Regelverk bör vara tydliga, kommunicerbara och, om så är möjligt, teknikoberoende för att fungera över tid. Vaggeryds Kommun ska ha ett beslutat regelverk för informationsstruktur (klassificeringsstruktur).

Genom informationshangeringsplan ska respektive styrelse/nämnd, besluta om hur de förvaltar sin struktur för verksamhetstyp, verksamhetsområde, processer och information kopplat till dessa. Informationstillgångar ska vara identifierade och dokumenterade. I informationshangeringsplanen ska det också framgå hur information ska sparas alternativt gallras efter gällande lagstiftning.

Vaggeryds kommun ska bedriva verksamhetsdriven informationssäkerhet vilket innebär att verksamheterna har ansvar för sin informationssäkerhet och har bästa kunskap om hur känslig och kritisk verksamhetens information är, och därmed

bestämma informationens skyddsvärde. Verksamheten ska tillämpa regelverk för informationsklassning med syfte att ge känslig och kritisk information ett starkare skydd än annan information.

Informationen och informationsbärare (t.ex. system) ska klassas baserat på interna och externa krav på informationens **konfidentialitet, riktighet, tillgänglighet och spårbarhet**.

Vaggeryds Kommun ska tillämpa en enhetlig modell för informationsklassning.

Ansvar

Allmänt

För att bedriva ett framgångsrikt informationssäkerhetsarbete måste det vara tydligt vem eller vilka som har ansvar för det. Detta gäller på alla nivåer – både inom den egna organisationen och inom kommunkoncernen. Arbetet ska utgå ifrån att alla anställda och förtroendevalda vet vad det egna ansvaret omfattar och ha god kunskap om vilka säkerhetsregler som gäller. Detsamma gäller när tillfällig eller extern personal anlitas. Det är viktigt att alla (anställda och förtroendevalda) har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka informationssäkerheten.

Grundprincip kring ansvar

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från politisk ledning, kommunledningen till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt osv.) också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens informationssäkerhetssamordnare (CISO) och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till medarbetare, verksamheter och kommunens ledning, att kunna ta ansvaret för informationssäkerheten.

Övergripande ansvar

- Kommunfullmäktige fastställer övergripande mål och inriktning för informationssäkerhet genom en kommunövergripande informationssäkerhetspolicy.
- Kommunstyrelsen ansvarar för samordningen av informationssäkerhetsarbetet i kommunen och ska därför årligen fastställa en övergripande handlingsplan för informationssäkerhetsarbetet.
- Kommundirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunfullmäktiges fastställda informationssäkerhetspolicy. Kommundirektören fastställer, på delegation av kommunstyrelsen, kommunövergripande riktlinjer för informationssäkerhet.

- Chefer inom Vaggeryds kommun ansvarar för att medarbetare i Vaggeryds kommun efterlever informationssäkerhetspolicyn och riktlinjer för informationssäkerhet. Ledningen bör visa sitt stöd för dessa dokument och fungera som förebild.

Ansvar inom respektive verksamhet

- Varje styrelse/nämnd är ansvarig för informationssäkerheten inom sitt verksamhetsområde. Styrelse/nämnd kan vid behov besluta om instruktioner som kompletterar de centrala riktlinjerna för informationssäkerhet.
- Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Det åligger varje verksamhetsansvarig att se till att sina medarbetare efterlever riktlinjer, har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås. Säkerhetsansvaret i sig kan inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

Medarbetares ansvar

- Alla medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler, rapportera informationssäkerhetsrelaterade brister och incidenter. Om någon enskild befattningshavare ändå bryter mot gällande styrdokument bär vederbörande själv ansvaret för sitt handlande.