HÖGSBY KOMMUN

INFORMATIONS-SÄKERHETSPOLICY

Högsby kommun 2020 - 2022

SAMMANFATTNING

Information är en grundläggande byggsten i en organisation, på samma sätt som medarbetare, lokaler och utrustning. En del av vår information är värdefull, både för organisationer och för den enskilda människan, och kan ibland till och med vara livsviktig såsom informationen i patientjournaler. Är den informationen förlorad eller felaktig kan det få katastrofala följder. Information i sig utgör därför en av kommunens absolut viktigaste tillgångar.

Jonas Högquist

Dokumenttyp Policy	Dokumentnamn Informationssäkerhetspolicy Högsby kommun	Beslutad/Antagen KF 2020-06-08 (KF § 81 KU.2020.138)	Version 1.0
Dokumentägare Kommunfullmäktige	Dokumentansvarig Informationssäkerhetssamordnare	Reviderad	Giltighetstid 2020–2022

Innehållsförteckning

Inledning

Bakgrund

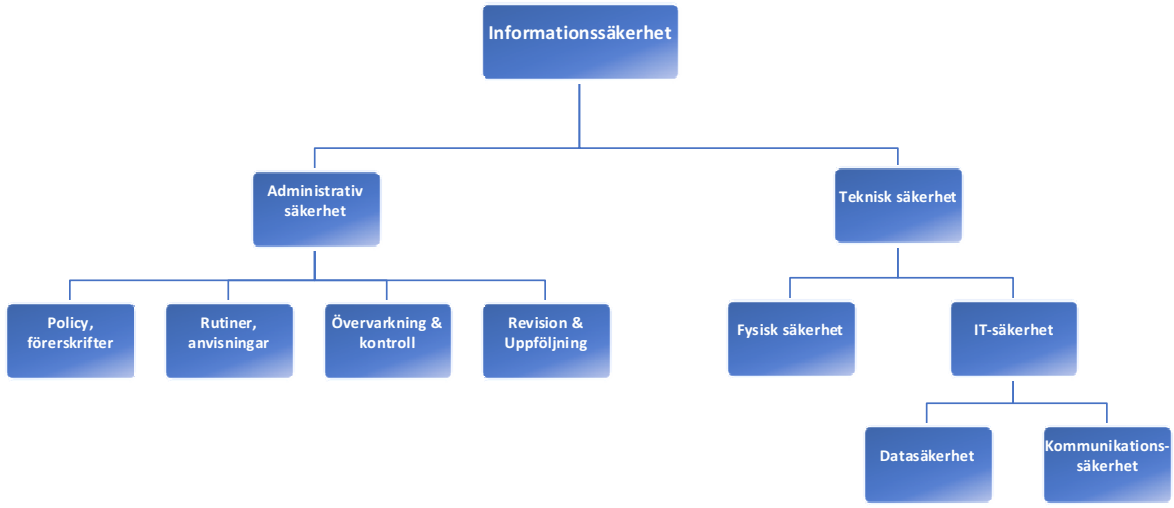
Information är en grundläggande byggsten i en organisation, på samma sätt som medarbetare, lokaler och utrustning. Information är medlet för att förmedla kunskap. Vi kan kommunicera information, vi kan lagra den, vi kan förädla den och vi kan styra processer med den – vi behöver den för det mesta vi gör helt enkelt. En del av vår information är värdefull, både för organisationer och för den enskilda människan, och kan ibland till och med vara livsviktig såsom informationen i patientjournaler. Är informationen förlorad eller felaktig kan det få katastrofala följder och medföra stora ekonomiska förluster. Information i sig utgör därför en av kommunens absolut viktigaste tillgångar.

Brister i hantering av information leder till ett försämrat förtroende för kommunala tjänster och verksamheter. Allvarliga och upprepade störningar kan leda till förtroendekriser, som också kan sprida sig till fler verksamheter och tjänster och även till andra sektorer i samhället.

Genom ett systematiskt arbete med informationssäkerhet kan Högsby kommun öka kvaliteten i och förtroendet för den kommunala verksamheten. Invånare, företagare, organisationer och övriga intressenter ska känna sig trygga i kontakten med Högsby kommun och vara säkra på att personuppgifter och andra informationstillgångar hanteras på ett tillförlitligt sätt.

Informationssäkerhet

Arbetet med informationssäkerhet består av att införa och förvalta administrativa regelverk så 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.



Vi behöver 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 (konfidentialitet)

Kraven på hantering av information styrs förutom av lagar, förordningar, föreskrifter och avtal också av de kommunala verksamheternas krav på funktion och tillämplighet, samtidigt som den enskilde,

företag och andra aktörer i vår omvärld naturligtvis också har behov och förväntningar som ställer krav på vår informationssäkerhet. Informationssäkerhetsskyddet behöver således anpassas efter behovet så att det är tillräckligt bra och inte för svagt eller alltför krångligt och dyrt.

Informationssäkerhetspolicyns ändamål

Informationssäkerhetspolicyn är ett strategiskt dokument och redovisar kommunfullmäktiges övergripande mål och viljeinriktning för informationssäkerhetsarbetet i Högsby kommun samt hur ansvaret i dessa frågor är fördelade.

Övergripande målsättning

Målet med informationssäkerhetsarbetet är att hantera och skydda informationen i verksamheterna på sådant sätt att rättsliga och verksamhetsmässiga krav samt invånarintressen kan tillgodoses, samtidigt som informationssäkerhetsarbetet även främjar verksamheternas funktionalitet, kvalitet och effektivitet och tillgodoser invånarens rättigheter och personliga integritet.

Strategiska målsättningar

Effektmål

- Genom ett strategiskt informationssäkerhetsarbete främja Högsby kommuns förmåga att förebygga och hantera allvarliga störningar och kriser.
- Verka för att samtliga anställda och förtroendevalda inom Högsby kommun ska känna till och följa kommunens policys, riktlinjer och instruktioner inom informationssäkerhet.
- Invånare, företagare och övriga intressenter ska känna sig trygga i kontakten med Högsby kommun och vara säkra på att personuppgifter och andra informationstillgångar hanteras på ett tillförlitligt sätt.

Resultatmål

- Arbeta systematiskt för att säkerställa att kunskap om informationssäkerhet och dess innebörd ska finnas i organisationen.
- Att systematiskt klassificera informationstillgångar utifrån verksamheternas krav på konfidentialitet, riktighet och tillgänglighet.
- Systematiskt arbeta för att skyddet ska vara anpassat till informationens skyddsvärde, risk och lagkrav och därigenom möjliggöra för kommunens verksamheter att uppnå sina mål.

Principer och arbetssätt

Högsby kommun ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet ska gentemot koncernens verksamheter vara normerande, stödjande och kontrollerande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande kommunens informationstillgångar, samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Högsby kommun ska:

- vara systematiskt och bygga på etablerade standards (ISO 27000). Systematiken innebär kontinuerliga uppföljningar med reviderade handlingsplaner enligt metodiken planera, genomföra, följa upp och åtgärda.
- utifrån återkommande risk-och sårbarhetsanalyser och inträffade incidenter, vidta nödvändiga åtgärder (planeras och dokumenteras i handlingsplan) för att se till att vår information har rätt skydd. Skyddsåtgärder ska vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en otillräcklig säkerhet kan medföra.
- ställa säkerhetskrav inför upphandling, utveckling, användning och avveckling av informationstillgångar och uppföljning av ställda krav ska ske kontinuerligt.
- ska utgå från kontinuitetsplanering och ha beredskap för avbrott och störningar. Våra kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av incidenter.
- 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.
- säkerställa rätt identitet och behörighet utifrån roll, för alla som får tillgång till information. Det gäller vid nytt, ändrat eller avslutat behov.
- utgå ifrån att alla informationstillgångar är identifierade och dokumenterade. Hantering av personuppgifter ska följa särskilda riktlinjer. All information ska sparas, alternativt gallras, enligt gällande lagstiftning och finnas dokumenterat.

Verksamhetsdriven informationssäkerhet

Verksamheterna har ansvar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras information är, och därmed kunskap om informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheterna, utifrån informationens skyddsvärde, ställer krav på de aktörer som hanterar informationen, exempelvis användare, systemansvariga samt drifts-och systemleverantörer.

För detta ändamål ska informationsklassning tillämpas, där information klassas med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Därigenom kan en anpassad och effektiv informationssäkerhet skapas. Informationen ska systematiskt definieras och värderas (enligt SKRs ”KLASSA”).

Högsby kommun ska tillämpa en enhetlig klassningsmodell för att värdera informationstillgångar. Informationstillgångar består av information och resurser som används för att hantera information, exempelvis IT-system, IT-infrastruktur och fysiska tillgångar. Själva informationen är den primära tillgången som ska klassas i det första ledet. 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 klassningsmodellen beskriver och som anger olika nivåer av skyddskrav baserat på interna och externa krav på informationens konfidentialitet, riktighet, tillgänglighet.

Organisation, ansvar och roller

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Det gäller från koncernledning till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens informationssäkerhetssamordnare och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhetsansvaret.

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvar och tillhörande uppgifter för respektive roller beskrivs utförligare i riktlinjer inom informationssäkerhetsområdet.

Kommunfullmäktige fastställer informationssäkerhetspolicyn som ska gälla för Högsby kommun.

Kommunstyrelsen har det övergripande ansvaret för informationssäkerheten i Högsby kommun.

Informationssäkerhetssamordnare har det övergripande ansvaret för att leda, samordna och utveckla det strategiska informationssäkerhetsarbetet.

Dataskyddsombud har uppdraget att ge information, rådgivning och utbildning samt skapa och tillhandahålla mallar. Dataskyddsombudet kontrollerar att bestämmelserna om dataskydd efterlevs och fungerar även som kontaktperson mot tillsynsmyndighet (Datainspektionen).

Dataskyddssamordnare övervakar att organisationen följer dataskyddsförordningen, kontrollerar att organisationen följer interna styrdokument och fungerar som ett stöd till verksamheterna i deras arbete med dataskydd.

Kommunchefen har kommunstyrelsens uppdrag att se till så att informationssäkerhetsarbetet bedrivs så effektivt som möjligt i enlighet med denna policy och tillhörande riktlinjer.

Chefer på alla nivåer ansvarar för informationssäkerheten inom sin verksamhet. Varje chef ansvarar för att egna medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en nödvändig informationssäkerhet i verksamheten kan uppnås.

Systemägaren har det övergripande ansvaret för ett IT-system och är även ansvarig för all data i, eller exporterat från, informationstillgången. I ansvaret ingår även att tillgången efterlever informationssäkerhetspolicyn och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om tillgångens informationssäkerhetsnivå genom att klassning sker enligt beslutad modell. Systemägaren ska utse systemförvaltare och vid behov även informationsägare, samt säkerställa att avtal för personuppgiftsbiträde finns i de fall detta är aktuellt.

Systemförvaltare är den eller de personer i berörda verksamheter som har ansvaret för den dagliga användningen av systemet och tillser att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Informationsägare (oftast densamme som systemägare) är den som äger och ansvarar för att informationen är riktig, tillförlitlig och hanteras enligt kommunens policy, riktlinjer och rutiner samt att all relevant lagstiftning följs.

Informationsförvaltare (kan vara samma som systemförvaltare) är den som aktivt förvaltar informationen på informationsägarens uppdrag.

IT-strateg bidrar med ämneskunskap och stöd till verksamheterna i frågor som rör IT.

Arkivarie verkar för att information i kommunens system är åtkomlig för allmänheten enligt reglerna i offentlighets- och sekretesslagen (OSL) samt att den gallras och bevaras enligt beslut i dokumenthanteringsplaner.

Medarbetare och förtroendevalda ansvarar för att tillämpa gällande informationssäkerhetspolicy, riktlinjer och regler. Man har som medarbetare och förtroendevald ett ansvar att vara uppmärksam och rapportera händelser och avvikelser som kan påverka säkerheten, och aktivt verka för att förbättra säkerheten inom sin verksamhet.

Informationssäkerhetsrådet är en ledningsfunktion, bestående av representanter från kommunens olika verksamheter, som under ledning av informationssäkerhetssamordnare träffas regelbundet för att planera och följa upp informationssäkerhetsarbetet.

Uppföljning och rapportering

Uppföljning ska ske regelbundet och är en viktig del i informationssäkerhetsarbetet för att bevaka att beslutade åtgärder är genomförda, årliga mål är uppfyllda, regler efterlevs och att policydokument och systemsäkerhetsplaner vid behov revideras.

Informationssäkerhetssamordnare ska årligen rapportera läge och status gällande informationssäkerhet till kommundirektören och kommunstyrelsen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.