UTFÄRDARE Ali Ababneh			DOKUMENTTYP Policy	
BESLUTAD AV KOMMUNFULLMÄKTIGE	DIARE NUMMER KS 2023/68	DATUM 2023-04-17	VERSION 2.0	DOKUMENTIDENTIFIKATION

PROGRAM
Uttrycker värdegrund och önskvärd utveckling av verksamheten.

POLICY
Uttrycker ett värdegrundsbaserat förhållningssätt och principer för vägledning.

STRATEGI
Konkretiserar ett program eller en policy och utgör en grund för prioritering.

HANDLINGSPLAN
Beskriver konkreta mål och åtgärder.

RIKTLINJER
Säkerställer ett riktigt agerande och en god kvalitet vid handläggning och utförande.

Informationssäkerhetspolicy
Denna policy innehåller Haparanda kommuns viljeinriktning och övergripande mål för informationssäkerhetsarbetet som redovisar kommunens övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat. Samtliga nämnder och deras verksamheter omfattas av denna informationssäkerhetspolicy, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna. Policy för informationssäkerhet kompletterar övriga styrdokument bland annat IT, kvalitet, GDPR, kommunikation och övrig säkerhet.

Styrdokumentet riktlinjer för informationssäkerhet är mer detaljerat och konkretiserar denna informationssäkerhetspolicy.

Bakgrund
Information finns i alla kommunens verksamheter och handlar om allt det vi gör, exempelvis om vår personal, våra tjänster, vår ekonomi och det omgivande samhället med medborgare, företag, föreningar osv. Information är därför i sig en av kommunens viktigaste tillgångar.

Behovet av informationssäkerhet ökar i takt med att kommuninvånarna förväntar sig effektiv kommunikation via självbetjäning med hjälp av e-tjänster, samt i direktkontakt med kommunen. Även förvaltningarnas användning av systemstöd för att leverera tjänster på ett effektivt sätt ökar. Invånarna ska kunna förvänta sig att kommunen hanterar information som rör dem, exempelvis personuppgifter och information på ett säkert sätt. I samband med kriser krävs också effektiv och säker kommunikation med berörda verksamheter och invånare. Konsekvensen av bristande informationssäkerhet kan medföra störningar i samhällsviktiga verksamheter, att information går förlorad, förvanskas eller rent av stjäls. Det kan även medföra ekonomiska förluster och att förtroendet för eller varumärket Haparanda Stad påverkas negativt.

Informationssäkerhet
Informationssäkerhet omfattar hela kommunens verksamhet och all information utan undantag. Oavsett den hanteras i cyberrymden, i datorer, i ett telefonsamtal eller på ett papper. Då stora delar av informationen hanteras med hjälp av IT-system handlar informationssäkerhet även om teknik.

Med informationssäkerhet säkerställs följande
För att nå en hög kvalitet i vårt arbete måste information hanteras på rätt sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt rutiner och skydd av information utifrån fyra aspekter:

- **Riktighet** – Att information inte kan förändras av obehöriga, av misstag eller på grund av störningar i funktion/system. Informationen ska vara tillförlitlig, korrekt och fullständig.
- **Sekretess** – Att information i dokument, system och handlingar etc. med lagkrav om sekretess eller motsvarande inte görs tillgängliga eller avslöjas för obehörig.
- **Spårbarhet** – Att i efterhand kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt ex. handling, användare, dator, skrivare eller system/program.
- **Tillgänglighet** – Att information är tillgänglig i skälig och förväntad utsträckning och inom rimlig tid.

Övergripande målsättning
En god informationssäkerhet syftar till att säkerställa en effektiv informationsförsörjning och att minimera riskerna för fel som påverkar möjligheterna att bedriva en ändamålsenlig verksamhet. Arbetet med informationssäkerhet ska vara systematiskt och långsiktigt.

Genom ett systematiskt informationssäkerhetsarbete möjliggör att lagkrav kan följas, att samhällskritisk verksamhet kan upprätthållas, informationsläckage kan förhindras, kontroll av kostnader uppnås och att förtroendet för kommunens tjänster och varumärke skyddas.

Strategiska målområden

- Informationsförsörjningen ska vara säker, effektiv och bidra till stöd åt verksamheterna.
- Informationssäkerhetsarbetet ska vara systematiskt och bygga på de etablerade internationella informationssäkerhetsstandard SS-ISO/IEC 27001.
- Kommunövergripande rutiner, regler och anvisningar ska upprättas.
- Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckning ska framgå vem som är informations/system ägare och förvaltare.
- Genom klassificering värdera och prioritera informationstillgångar utifrån verksamhetens krav på riktighet, sekretess, spårbarhet och tillgänglighet.
- Personal ska ha kunskap om gällande informationssäkerhetsregler som rör det egna tjänstestället och de informationssystem/rutiner som där används.
- Informationssäkerhetsarbetet ska vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa
- För att ha förmåga att bedriva verksamheten på acceptabel nivå under normala förhållanden och vid kriser eller störningar ska kontinuitetsplanering genomföras för varje informationstillgång.
- Informationssäkerhetsarbetet ska ske i aktiv samverkan med det omgivande samhället såsom myndigheter, företag och nätverk, särskilt sådana som är normgivande inom informationssäkerhet som t.ex. SKR (Sveriges Kommuner och Regioner), MSB (Myndigheten för samhällsskydd och beredskap) och SIS (Swedish Standards Institute).
- Informationssäkerhetsarbetet ska vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa.
- Intern systematisk process för granskning och kontroll av IT-miljö, IT-nätverk, processer, system, infrastruktur med avseende på säkerhetsnivå ska genomföras en gång per år av en extern part och rapportera till kommunstyrelsen.

Verksamhetsdriven genom informationsklassning

Kommundirektören har det övergripande ansvaret för informationssäkerheten. Under Kommundirektören följer ansvaret linjeorganisationen. Verksamheter har ansvar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras informationsmängder är, och därmed informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheter utifrån informationens skyddsvärde ställer krav på de aktörer som hanterar informationen.

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.

Haparanda kommun ska tillämpa en enhetlig modell för informationsklassning som anger olika nivåer av skyddskrav vari information ska klassas baserat på interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Roller och ansvar
Grundprincipen är att ansvaret för informationssäkerheten 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 informationssäkerhetsansvarige och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet, cybersäkerhet eller andra relaterade frågor, fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhetsansvaret.

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvaret och tillhörande åligganden för respektive roller beskrivs utförligare i riktlinjer för informationssäkerhet.

Medarbetare har ett ansvar att följa Haparanda kommuns informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Man har som medarbetare också ansvar att vara uppmärksam på brister och incidenter rörande informationssäkerheten och meddela sådana till IT och närmsta chef.

Ledningar i form av kommunfullmäktige, kommunstyrelse, och nämnder har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom sina respektive verksamhetsområden.

Verksamhetsansvariga, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Det åligger varje verksamhetsansvarig att tillse att sina medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås.

Objektägare (operativ systemägare) ansvarar för att förvaltningsobjekt efterlever informationssäkerhetspolicy och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om objektets informationssäkerhetsnivå(-er) genom att klassning sker i enlighet med Haparanda kommuns modell för informationsklassning.

Systemanvändare Varje systemanvändare ansvarar för att ta del av och följa uppsatta regler för systemanvändning och systemsäkerhet.

Förvaltningschef ansvarar för att objekts informationssäkerhetsrelaterade mål och åtgärder nås respektive genomförs.

IT-enheten ansvarar för den dagliga IT driften och för att utveckla och implementera IT-strategier. Enheten ansvarar också för att säkerheten i Haparanda kommuns IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt denna informationssäkerhetspolicy och underliggande riktlinjer för informationssäkerhet.

IT-chef samordnar arbetet med säkerheten i Haparanda kommuns IT-miljö, har internt tillsynsansvar för att IT-miljön är tillförlitlig och motsvarar interna och externa krav, samt ansvarar för ledning och utveckling av IT och ser dessutom till att IT miljön är så säker.

Informationssäkerhetsansvarig har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Informationssäkerhetsansvarig ska arbeta i samråd med säkerhetsskyddschefen, IT-chefen och övriga ledamöter i kommunen.

Säkerhetsskyddschef/Säkerhetschef ansvarar för kontakter med myndigheter, fysisk säkerhet för kontor, rum och anläggningar samt regler för användning, skydd, giltighetstid för kryptografiska nycklar. Säkerhetschefen ansvarar även för att krisplanen följs och för att kalla till krisstabmöte enligt krisplanen vid behov.

Kommunstyrelsen har tillsynsansvar för att informationen hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen, samt kommunens interna styrdokument rörande informationens långsiktiga hantering och bevarande.

Dataskyddsombud, DSO
Dataskyddsombudet är en självständig och oberoende stöd- och kontrollfunktion. Dataskyddsombudets uppgifter är enligt dataskyddsförordningen bland annat att informera och ge råd om vilka skyldigheter som gäller enligt såväl dataskyddsförordningen som andra nationella dataskyddsbestämmelser, bevaka att dessa regler följs och ge råd om den konsekvensbedömning avseende dataskydd som ska göras enligt förordningen.

Personuppgiftsansvariga är kommunstyrelsen och övriga nämnder i kommuner. Dessa är ansvariga för hanteringen av personuppgifter och ska utse personuppgiftsombud som kontrollerar att personuppgifter hanteras på ett korrekt sätt i verksamheten.

Uppföljning och rapportering
Efterlevnaden av informationssäkerhetspolicyn och riktlinjer för informationssäkerhet ska följas upp regelbundet. Informationssäkerhetsansvarig 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.