NORDANSTIGS KOMMUN

Informationssäkerhetspolicy

Dokumentnamn Informationssäkerhetspolicy.docx			**Reviderad,** datum 2020-10-26 - - - - - - - - - - - - - - - - - -
Dokumentansvarig Morgan Norell	**Fastställd av** Kommunfullmäktige § 175, 2019-12-16 (KF § 60, 2020-10-26)		
Diarienummer 2019-000342	**Original** datum **2019-08-09**	**Giltig** till och med **2023-12-31**	

Inledning

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Nordanstigs kommun, inklusive de bolag, stiftelser och ekonomiska föreningar där kommunen utövar ett rättsligt bestämmande och/eller inflytande. Policyn ska även tillämpas av dem som har beroenden till kommunens gemensamma informationstillgångar.

Kommunens informationssäkerhetsarbete ska bedrivas på ett systematiskt, formaliserat och riskorienterat sätt och ta sin utgångspunkt i den internationella ledningssystemstandarden för informationssäkerhet, SS-ISO/IEC 27000.

Bakgrund

Behovet av informationssäkerhet ökar i takt med kommunens digitalisering. Digitalisering innebär för kommunen att information finns mer tillgänglig än tidigare, kommunen ska effektivt kunna kommunicera med medborgare, andra myndigheter och i den egna organisationen.

Informationssäkerheten begränsas inte till kommunens IT-system utan omfattar information i alla dess former och oavsett hur informationen lagras, bearbetas och kommuniceras.

Syfte

Det övergripande syftet med kommunens informationssäkerhetsarbete är att säkerställa ett väl avvägt skydd för kommunens informationstillgångar så att rätt information är tillgänglig för rätt person vid rätt tidpunkt och på ett spårbart sätt.

Informationssäkerhet

Denna policy omfattar alla informationstillgångar inom alla verksamheter utan undantag, oavsett om den behandlas manuellt eller automatiskt, och oberoende av i vilken form eller miljö den förekommer. All information ska vara klassificerad med avseende på känslighetsgrad.

Informationssäkerhetsarbetet ska ta sin utgångspunkt i regelbundna riskanalyser som syftar till att avväga rätt skyddsnivå i alla delar av verksamheten, samt motivera investeringar eller utbildningsinsatser för att säkerställa följande:

- *Konfidentialitet*: Förhindra eller försvåra för obehöriga att få tillgång till information, informationen åtkomstbegränsas
- *Riktighet:* Säkerställa att den information som produceras och bearbetas är tillförlitlig, aktuell och fullständig
- *Tillgänglighet:* Bidra till att informationen är åtkomlig vid behov, i förväntad utsträckning samt av rätt person med rätt behörighet
- *Spårbarhet:* Identifiering och autentisering av användare, samt loggning av relevanta händelser

För vart och ett av dessa områden ska organisatoriska, administrativa och tekniska skyddsåtgärder vidtas och dokumenteras på ett sådant sätt att det går att kontrollera att en tillfredsställande skyddsnivå uppnåtts.

Informationssäkerhetsskyddet ska granskas regelbundet. Avvikelser och incidenter ska systematiskt dokumenteras och följas upp, så att erfarenheter från dessa kan tas till vara som en del av det kontinuerliga förbättringsarbetet. Resultatet av säkerhetsarbetet ska årligen redovisas för kommunens ledningsgrupp.

Mål

Kommunens arbete med informationssäkerhet har som mål att:

- informationssäkerhet är en naturlig del i verksamheterna
- kunskap finns om hur informationssäkerheten säkerställs
- alla informationstillgångar är klassificerade
- hotbilder mot informationstillgångar fortlöpande analyseras
- händelser som kan leda till negativa konsekvenser förebyggs
- krishanteringsförmågan fortlöpande analyseras och upprätthålls

Organisation

Nedan är den organisation som har ansvar och styr kommunens informationssäkerhetsarbete.

Kommunfullmäktige uttrycker sin viljeinriktning i denna policy.

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhetsarbete.

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

Informationsägarna har det övergripande och yttersta ansvaret för respektive informationstillgång. Informationsägaren avgör vilken information som får hanteras, hur den hanteras och av vem. Informationsägarskapet följer verksamhetsansvaret.

Objektägarna, vanligtvis verksamhetschef/enhetschef, har övergripande ansvar för IT-systemen inom sitt objekt och dess användning. Objektägarna ansvarar för att systemen uppfyller informationssäkerhetskraven i förhållande till verksamhetens behov och hur informationstillgångarna klassificeras.

Förvaltningsledarna, vanligtvis medarbetare med systemansvar, har det funktionella, dagliga helhetsansvaret för ett förvaltningsobjekt. Förvaltningsledaren fungerar i hög grad som objektägarens utförare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Alla som hanterar informationstillgångar har ett ansvar att informationssäkerheten upprätthålls.

*objektsägare – Den person son ansvarar för att det finns adekvata system eller liknande som hanterar verksamhetens information. Objektsägaren ansvarar för att det finns adekvat skydd för den information som lagras eller bearbetas i systemet

*förvaltningsledare – Förvaltningsledare finns på beslutsnivån inom den objektnära förvaltningen och har uppdraget att förvalta it-systemen på objektsägarens uppdrag

*objekt – Med ett objekt menas ett it-system eller en samling av it-system som hanteras tillsammans. Det kan exempelvis vara vård och omsorgsobjektet där men då pratar om alla it-system för att sköta dessa verksamheter.

Efterlevnad

Kommunen ska följa lagar, författningar, avtalsförpliktelser samt andra säkerhetskrav enligt gällande rekommendationer om god informationssäkerhet.

Chefer inom kommunen ska säkerställa att alla säkerhetsrutiner inom deras respektive ansvarsområde utförs korrekt utifrån kommunens informationssäkerhetsregelverk.

Ytterligare information

För vidare information se dokument *Riktlinjer för informationssäkerhet.docx*