TIERPS KOMMUN

IT-säkerhetspolicy

Älvkarleby kommun | Knivsta kommun | Östhammars kommun – en del av Roslagen | Tierps kommun | Heby kommun

Dokumentets giltighet och beslut

Dokumentnamn:	IT-säkerhetspolicy
Gäller för:	Medlemskommuner i IT-nämnden
Gäller fr o m:	20ÅÅ-MM-DD
Gäller t o m:	20ÅÅ-MM-DD
Fastställd av:	KF Tierp § xx/2024, KF Heby § xx/2024, KF Knivsta § xx/2024 KF Älvkarleby § xx/2024, KF Östhammar § xx/2024
Fastställd:	20ÅÅ-MM-DD
Diarienummer:	ITN/2024:9

Dokumentansvar och handläggning

Dokumentansvarig:	Anne Eriksson, verksamhetschef Gemensam service
Handläggare:	Magnus Larsson, förvaltningschef IT

Dokumenthistorik

Tidigare beslut:

Upphäver:

Innehållsförteckning

Inledning

IT-säkerhetspolicyn är IT-centrums övergripande styrdokument för IT-säkerhetsarbetet. Policyn beskriver bland annat fördelningen av ansvar för IT-säkerhetsarbetet och hur informationsteknik ska användas på ett säkert sätt inom IT-nämndens ansvarsområde.

Syfte

IT-säkerhetspolicyn syftar till att säkerställa att IT-centrum skyddar och hanterar all information och infrastruktur på ett säkert och strukturerat sätt i enlighet med gällande krav, inklusive IT-säkerhetsstandarder och andra kommunala regleringar. Policyn är utformad för att följa tillämpliga svenska och europeiska lagar samt garantera skyddet av konfidentialitet, integritet och tillgänglighet för all information som hanteras inom IT-centrums miljö.

Denna policy gäller uteslutande för IT-centrums infrastruktur och den data som hanteras inom dess IT-miljö. För slutanvändarutrustning, såsom mobiltelefoner, surfplattor, arbetsdatorer och AV-utrustning, gäller respektive medlemskommuns styrdokument för informationssäkerhet.

Omfattning

Denna policy gäller för IT-säkerheten inom IT-nämndens ansvarsområde och kompletterar nämndens och kommunernas övriga styrdokument inom säkerhetsområdet.

Ansvar och roller

IT-säkerhetsansvarig: Innehar ansvaret för att implementera och övervaka IT-säkerhetsåtgärder inom IT-centrum i enlighet med gällande regulatoriska krav och standarder. Arbetet utförs på uppdrag av IT-centrums informationssäkerhetschef (CISO).

Informationssäkerhetschef (CISO): Bär det övergripande ansvaret för utveckling, implementering och övervakning av IT-centrums informationssäkerhet.

Användare: Samtliga medarbetare, inklusive konsulter och annan resurspersonal vid IT-centrum, är skyldiga att efterleva denna policy.

Systemägare: Ansvarar för säkerheten i specifika system eller applikationer, inklusive genomförande av riskbedömningar och hantering av åtkomstkontroll.

IT-nämnden: Styr IT-säkerhetsarbetet, fattar beslut om IT-säkerhetspolicyn samt följer upp revisioner avseende IT-säkerhet. Nämnden ansvarar även för att säkerställa adekvat resursallokering för att upprätthålla och förbättra IT-säkerheten.

Informationsägare: informationsägare inom IT-centrum och medlemskommunerna har ansvaret för att klassificera och vidta åtgärder för att

skydda den information de äger samt säkerställa att informationsresurser hanteras enligt gällande lagstiftning, regulatoriska krav och interna riktlinjer. Informationsägare har även ansvar att medverka i riskbedömningar, samt godkänna eller avvisa behörighetsförfrågningar för åtkomst till deras information.

Leverantörer: Leverantörer som tillhandahåller tjänster, system eller support till IT-centrum och dess medlemskommuner har ansvar att följa de säkerhetskrav som ställs i denna policy, kravställning, och övriga relevanta styrdokument som är relevanta för uppdraget.

Externa parter: Externa parter med tillgång till tjänster, system, eller support från IT-centrum och dess medlemskommuner har ansvar att följa de säkerhetskrav som ställs i denna policy, relevanta styrdokument, och övriga instruktioner IT-centrum lämnar som villkor för tillgång och åtkomst.

Riskhantering

IT-centrum ska regelbundet, i enlighet med etablerade rutiner och processer, genomföra riskanalyser och riskbedömningar för att identifiera potentiella hot och sårbarheter i IT-miljön. Dessa analyser ska utföras minst årligen samt vid betydande förändringar i IT-infrastrukturen.

Åtgärder för att reducera eller mitigera identifierade risker ska implementeras och dokumenteras. Detta arbete kan genomföras internt inom IT-centrum och/eller i samverkan med externa samarbetspartners, medlemskommuner samt tillhörande kommunala bolag och stiftelser.

Resultaten av riskhanteringsarbetet ska dokumenteras och rapporteras till IT-nämnden, IT ledningsgrupp och medlemskommunerna för att säkerställa adekvat åtgärdsplanering och resursallokering.

Åtkomstkontroll

Samtliga användare ska tilldelas en unik identifiering och ett lösenord som följer fastställda standarder och rutiner för användning av IT-resurser inom medlemskommunerna samt tillhörande kommunala bolag och stiftelser.

Tilldelning av åtkomst ska ske i enlighet med principen om minsta privilegium, vilket innebär att en användare endast ska ha tillgång till de resurser som är nödvändiga för att utföra sina arbetsuppgifter.

För särskilt känsliga system och data ska multifaktorautentisering implementeras.

Användarbehörigheter ska granskas och revideras regelbundet, minst en gång per år eller vid väsentliga förändringar i användarens roll eller anställning. IT-centrum ansvarar för att ta fram underlag och tekniska förutsättningar för att granskning och revision av behörigheter kan ske. Informationsägare hos medlemskommunerna ansvarar för att granskningen sker. Förändringar i användares behörigheter som hänger samman med avslut eller förändringar i uppdrag ska meddelas i god tid

innan uppdragets avslut enligt respektive medlemskommuns offboardingprocess. Otillbörlig åtkomst och incidenter som rör bristande avveckling av användarbehörigheter eller missbruk av behörigheter ska omedelbart anmälas till IT-säkerhetsansvarig.

Informationsskydd

IT-centrum ska säkerställa att all data hanteras med adekvata skyddsåtgärder för att förebygga intrång, dataförlust och otillbörlig manipulation.

All information ska klassificeras av respektive informationsägare och hanteras i enlighet med gällande lagstiftning, regulatoriska krav samt sekretesskrav.

Medlemskommunerna bär ansvaret för att all deras information säkerhetsklassificeras och tilldelas ett skyddsvärde baserat på Konfidentialitet (K), Riktighet (R) och Tillgänglighet (T).

Incidenter och säkerhetsöverträdelser som härrör hos leverantörer och kommuner, och påverkar IT-centrum, ska omgående rapporteras till IT-säkerhetsansvarig hos IT-centrum enligt fastställda rutiner. Inkomna ärenden ska hanteras enligt gällande processer med återrapportering till berörda intressenter.

Incidenter som härrör hos IT-centrum ska omgående rapporteras till verksamhetsansvarig chef, informationsägare, dataskyddsombud, eller informationssäkerhetsansvarig enligt respektive medlemskommuns rutiner.

IT-centrum ska genomföra regelbundna säkerhetskopieringar av all kritiska data och testa återställningsprocessen minst en gång per år för att säkerställa datas integritet och tillgänglighet.

Uppdatering och underhåll

IT-resurser, inklusive maskinvara och programvara, ska regelbundet uppdateras, underhållas och avvecklas för att säkerställa att verksamhetens information är skyddad mot kända sårbarheter. Kritiska säkerhetsuppdateringar ska installeras inom 30 dagar från utgivningsdatum, om inte särskilda omständigheter föreligger.

Eventuella avsteg från ovanstående ska dokumenteras som ett tidsbestämt undantag som ska godkännas av IT-centrum i samarbete med IT-säkerhetsansvarig.
IT-centrum ska upprätthålla en aktuell systemkatalog över alla IT-resurser, inklusive maskinvara, programvara och licenser, för att underlätta effektiv hantering och uppdatering.

Utbildning och medvetenhet

Anställda ska erhålla utbildning i IT-säkerhet och vara medvetna om potentiella hot och bästa praxis för att förebygga säkerhetsincidenter. Alla anställda ska genomgå

en grundläggande IT-säkerhetsutbildning årligen, medan personal med högre behörigheter ska få ytterligare specialiserad utbildning.

Utbildningen ska omfatta områden som allmän IT-säkerhetsmedvetenhet, lösenordshantering, dataskydd och GDPR, säker användning av företagsresurser, säker e-posthantering, säkerhetsmedvetenhet i sociala medier, fysisk säkerhet, säkerhet vid trådlös kommunikation, säkerhetsincidentrapportering och uppdateringar av programvara.

Effektiviteten av utbildningsinsatserna ska mätas genom regelbundna utvärderingar och simulerade phishing-tester, med resultaten rapporterade till ledningsgruppen för kontinuerlig förbättring av utbildningsprogrammet.

Respektive medlemskommun, kommunalt bolag och stiftelse ansvarar för att utbilda sin personal inom ramen för deras informationssäkerhetsarbete.

Följa lagar och standarder

IT-centrum ska följa alla tillämpliga nationella och internationella lagar och regler inom området IT-säkerhet. Detta inkluderar, men är inte begränsat till, GDPR, NIS2-direktivet och andra relevanta cybersäkerhetsregleringar.

IT-centrum strävar efter att uppfylla relevanta ISO-standarder för IT-säkerhet, särskilt ISO 27001 och ISO 27002.

IT-centrum ska genomföra årliga granskningar av regelefterlevnad och vidta nödvändiga åtgärder för att säkerställa kontinuerlig överensstämmelse med gällande lagar och standarder.

Revision av policyn

IT-säkerhetspolicyn ska regelbundet granskas av IT-säkerhetsansvarig för att säkerställa dess relevans och effektivitet. Om inget behov av revidering uppstår gäller policyn tre år i taget. Eventuella förändringar ska delges medlemskommunerna som ska vara delaktiga i remissarbetet inför nytt beslut i respektive fullmäktige.

Rapportering av överträdelser

Överträdelser av denna policy eller säkerhetsincidenter ska omedelbart rapporteras till IT-säkerhetsansvarig. Rapportering ska ske enligt en fastställd incidenthanteringsprocess, som inkluderar eskalering till lämplig ledningsnivå beroende på incidentens allvarlighetsgrad.

Denna IT-säkerhetspolicy ska betraktas som styrande för IT-centrums infrastruktur. Efterlevnad av denna policy är avgörande för att skydda IT-centrums och IT-nämndens medlemskommuners information och IT-resurser från hot och risker.