Program Plan Policy Riktlinje

Riktlinje för informationssäkerhet - fysisk och teknisk säkerhet

Beslutad av: Kommunstyrelsen
Datum och paragraf: 2023-10-03, § 192
Dokumentansvarig: Administrativ chef
Revisionsdatum:
Dnr: 23KS48

Innehåll

1 Inledning

Information är en viktig tillgång och en förutsättning för att kommunen ska kunna bedriva verksamhet. Kommunens informationstillgångar måste därför hanteras på ett tillfredsställande sätt utifrån tre informationssäkerhetsaspekter:

- att information enbart är tillgänglig för behöriga (konfidentialitet)
- att information är korrekt, aktuell och fullständig (riktighet)
- att information är åtkomlig i rätt tid och användbar (tillgänglighet)

Detta dokument vänder sig till de som i Askersunds kommun ansvarar för informationstillgångar och att dessa utifrån informationens skyddsvärde har ett relevant fysiskt och tekniskt skydd. Dokumentet är på övergripande nivå varför kompletterande och mera detaljerade rutiner är nödvändiga. Dessa upprättas av respektive verksamhet samt i avtal med driftsleverantörer. Som stöd för detta dokument används hänvisningar till standarder för informationssäkerhet.

2 Avtal

2.1 Tjänsteleverantörer

Ett av syftena med denna riktlinje är att ge stöd för kravställning avseende fysisk och teknisk säkerhet för informationstillgångar som hanteras av externa tjänsteleverantörer. Kraven ska beskrivas och regleras i avtal med respektive leverantör. Leverantören ska ha kvalitetsledningssystem där man beskriver hur arbetet ska utföras och den fysiska och tekniska säkerheten upprätthållas.

3 Styrning av åtkomst

Styrning av åtkomst syftar till att begränsa åtkomst till informationstillgångar och resurser som hanterar dessa.

Informationsägaren ska säkerställa att det finns relevanta regler för åtkomst, rättigheter och begränsningar för olika roller/befattningar. Principer för tilldelning av behörigheter bygger på informationstillgångens skyddsbehov och rollers/befattningars behov för att kunna utföra sina arbetsuppgifter.

Rutiner ska finnas för styrning av de behörigheter som kommunen ansvarar för. Rutiner ska även finnas för omflyttning och överlåtelse av utrustning till annan användare.

Användares åtkomst till systemfunktioner och information ska styras på en så detaljerad nivå som möjligt i avsikt att begränsa risken för oegentligheter.

3.1 Hantering av användaråtkomst

Personliga användarkonton och lösenord ska skapas enligt fastställd rutin för registrering, ändring och avregistrering för respektive system.

Gruppkonton får inte användas på grund av att spårbarhet då inte kan säkerställas. Avsteg från detta kan enbart beslutas av förvaltningschef.

3.2 Åtkomst till resurser som hanterar informationstillgångar

Kraven på styrning av behörigheter gäller även tillgång till resurser som hanterar informationstillgångar.

Endast särskilda behöriga ska ha åtkomst till och behörighet att administrera resurser som hanterar informationstillgångar. Rutiner ska finnas för att säkerställa behörigheten.

Tilldelning och förändring av åtkomsträttigheter ska beslutas av informationsägaren.

Leverantörslösenord och behörigheter (till exempel applikationer, databaser och servrar) ska ändras vid leverans och förvaras inlåsta.

3.3 Uppföljning av användares åtkomsträttigheter

Objektsägaren ska fastställa rutiner för regelbunden uppföljning av användarkonton och tilldelade behörigheter. Denna kontroll ska dokumenteras och rapporteras till informationsägaren.

4 Kryptering

Syftet med kryptering är att skydda informationens tillgänglighet, riktighet och konfidentialitet.

Bedömning kring behov av kryptering ska baseras på informationens skyddsvärde.

Tjänsteleverantörer ska kontaktas om behov av kryptering finns. Införande av krypteringslösningar medför krav på rutiner om nyckelhantering, utbildning och resurser.

5 Fysisk och miljörelaterad säkerhet

Informationstillgångar och utrustning ska ha ett grundläggande skydd för att förhindra otillåten fysisk åtkomst, skador eller störningar:

- lokaler ska utformas utifrån informationstillgångarnas skyddsvärde
- lokaler bör vara fysiskt skyddade mot naturkatastrofer, illvilliga angrepp, brand och stöld genom separering och larm
- fysiska avgränsningar och tillträde ska anpassas efter skyddsvärdet på informationstillgången
- vid behov ska överspänningsskydd och reservkraft användas som skydd för att förändringar i elförsörjningen inte ska påverka den tekniska infrastrukturen
- kylanläggning kan behövas för att säkerställa rätt driftstemperatur
- rutiner för testkörning av reservkraft och kylning ska finnas

5.1 Säkra områden

Objektsägaren ska i samråd med informationsägare definiera fysiska avgränsningar för de områden som behöver skyddas och upprätta besöksrutiner. Utformningen ska anpassas utifrån informationens och utrustningens skyddsvärde. Vem som har mandat att besluta om besök i utrymmen med särskilt skyddsvärd information eller utrustning ska vara dokumenterat.

5.2 Fysiskt skydd för utrustning som hanterar informationstillgångar

Objektsägare ska tillsammans med informationsägare utarbeta rutiner för att hantera skyddsvärd utrustning.

Rutiner ska omfatta beslut om var utrustning får placeras, tekniska försörjningssystem, kablagesäkerhet, underhåll av utrustning, mobila enheter, utförsel av tillgångar, säkerhet för utrustning och tillgångar utanför organisationens lokaler, säker kassering eller återanvändning.

Installation och konfiguration av medarbetares datorer och annan kringutrustning hanteras av Sydnärke-IT.

Enbart godkänd utrustning får kopplas in i nätverket. Medarbetares hantering av utrustning framgår i riktlinjer informationssäkerhet för medarbetare.

6 Driftssäkerhet

Rutiner för driftssäkerhet syftar till att säkerställa korrekt och säker drift av all utrustning som hanterar informationstillgångar.

6.1 Drift

All utrustning som hanterar informationstillgångar ska ha dokumenterade driftsrutiner. Serviceavtal (SLA) bör upprättas med driftsleverantörer och ska innehålla uppsatta mål för vad driftleverantören ska prestera och hur dessa följs upp.

6.2 Hantering av tekniska sårbarheter

Genom omvärldsbevakning och leverantörskontakter kan information om tekniska sårbarheter bli kända. Åtgärder för att eliminera dessa ska vidtas så snart som möjligt.

6.3 Ändringshantering

Rutiner ska finnas för ändringshantering vid förändringar i exempelvis organisation, verksamhetsprocesser, system eller utrustning som kan påverka drift och/eller informationssäkerhet. Riskanalyser ska genomföras och förändringen planeras.

6.4 Skydd mot skadlig kod

Skydd mot skadlig kod ska finnas och användas tillsammans med rutiner för hur användare ska agera och rapportera vid ett angrepp.

Verksamhetssystem, servrar, datorer och mobila enheter ska vara uppdaterade enligt tjänsteleverantörernas krav.

6.5 Säkerhetskopiering

Objektsägaren ska i samråd med informationsägare och driftsleverantör upprätta rutiner för säkerhetskopiering och återställning av information och system. Kraven på säkerhetskopiering och återställning ska framgå av driftsavtal och/eller objektplan. Återställningstester ska genomföras.

6.6 Övrigt

För att lösa vissa dator-/applikationsproblem kan driftsleverantören behöva ta över och fjärrstyra en dator. Detta får enbart ske när användaren har godkänt detta.

7 Nätverkssäkerhet

Nätverkssäkerhet innebär att skyddet av informationstillgångar i nätverk och kringutrustning till nätverk som används för att datakommunikation säkerställs.

7.1 Hantering

Skyddsåtgärder ska införas för att nå säkerhet för informationstillgångar i nätverk och anslutna tjänster utifrån informationens skyddsvärde.

Skydd för nätverkssäkerhet kan exempelvis vara:

- kryptering
- regler för nätverksanslutning

- begränsning av systemanslutningar
- brandväggar och intrångsdetekteringssystem
- loggning och övervakning av nätverk
- separation av nätverk (segmentering).

Kraven på skydd ska inkluderas i avtal med leverantörer av nätverkstjänster.

7.2 Informationsöverföring

Information som hanteras i e-post, systemintegration eller andra metoder för informationsöverföring ska ges lämpligt skydd.

Om information med höga skyddskrav avseende konfidentialitet ska sändas till extern part ska lösning för säker överföring med kryptering och signering användas. Säker överföring av verksamhetsinformation ska beskrivas och regleras i avtal mellan kommun och extern part.

8 Anskaffning, utveckling och avveckling av informationssystem

Relevant informationssäkerhet för system ska säkerställas över hela livscykeln.

8.1 Anskaffning och utveckling

Informationssäkerhetsklassificering ska göras inför anskaffning och utveckling av system.

Informationssäkerhetskrav ska dokumenteras och granskas av berörda parter innan anskaffning eller utveckling påbörjas. Anskaffning eller förändring av system ska involvera parterna i systemets förvaltningsorganisation.

Informationssäkerhetskrav ska omsättas i rätt tekniska krav så att system och information ges skydd som överensstämmer med skyddsvärdet.

Anskaffning eller förändring av underliggande IT-resurser i form av infrastruktur, stödsystem med mera ska ha minst motsvarande krav som de system de stödjer.

Avtal med driftsleverantör ska reglera ansvar för

- implementation och upprätthållande av säkerhetsfunktioner
- testning och verifiering av dessa
- brister som eventuellt upptäcks under drift

I kravspecifikationer ska alltid ställas tydliga krav på säkerhet. Upphandling av IT-stöd ska alltid göras i samverkan med upphandlingsenheten och objektledare-IT.

Vid upphandling av molnbaserade tjänster ska särskild vikt läggas vid säkerhetskraven och värdera om molntjänstlösning är lämpligt eller inte.

8.2 Avveckling

IT-system som inte längre behövs för verksamheten ska snarast avvecklas efter att informationen är omhändertagen. Objektsägaren fattar beslut om avveckling. Rutiner för avveckling ska utformas av respektive verksamhet och informationen ska hanteras enligt dokumenthanteringsplan.

9 Informationssäkerhet avseende verksamhetens kontinuitet

Informationsägare ska ta fram kontinuitetsplaner i syfte att hantera störningar/avbrott i verksamheten. Störningar och avbrott i verksamheten ställer stora krav på personal då svåra och snabba beslut ska fattas i en pressad situation. Planen ska bland annat innehålla analys om hur störningar/avbrott

påverkar verksamheten, vilka alternativa arbetssätt som ska användas samt vad som ska prioriteras och av vem.

Kontinuitetsplanen ska bygga på en riskanalys gjord utifrån informationssäkerhetskrav och bör med fördel integreras i övergripande kontinuitetsplan.

Tjänsteleverantören ska upprätta avbrottsplan som anger hur denne ska agera vid störningar/avbrott i IT-resurser. Krav på avbrottsplan ska framgå i avtalet med driftsleverantören.

10 Efterlevnad

Uppföljning av informationssäkerhet ska ske för att kontrollera tillräcklig säkerhetsnivå.

Kontroll och uppföljning ska genomföras av informationstillgångar med höga skyddsvärden. Rapportering av större sårbarheter och brister ska ske till informationsägare och kommunens krisberedskapssamordnare. Rutinen för säkerhetsincidentsrapportering ska följas.