Informationssäkerhet, fysisk och teknisk säkerhet - riktlinje



Beslutad av kommunstyrelsen 2024-03-06

Dokumentinformation

Fastställt av:	Kommunstyrelsen
Fastställt, datum:	2024-03-06
Dokumentsansvarig:	Chef säkerhetsenheten
Ansvarig för revidering:	Informationssäkerhetssamordnare
Gäller för:	Informationsägare och systemägare
Gäller till, datum:	Gäller tills vidare. Uppdateras vid behov.

Innehållsförteckning

Dokumentinformation 2
Informationssäkerhet, fysisk och teknisk säkerhet – riktlinje 4
1 Inledning 4
2 Avtal med driftsleverantörer 4
3 Styrning av åtkomst 5
3.1 Hantering av användaråtkomst 5
3.2 Åtkomst till resurser som hanterar informationstillgångar 5
3.3 Uppföljning av användares åtkomsträttigheter 5
4 Kryptering 6
5 Fysisk och miljörelaterad säkerhet 6
5.1 Säkra områden 6
5.2 Fysiskt skydd för utrustning som hanterar informationstillgångar 6
6 Driftssäkerhet 7
6.1 Drift 7
6.2 Hantering av tekniska sårbarheter 7
6.3 Ändringshantering 7
6.4 Utveckling och test 7
6.5 Skydd mot skadlig kod 7
6.6 Säkerhetskopiering 8
6.7 Övrigt 8
7 Kommunikationssäkerhet 8
7.1 Hantering av nätverkssäkerhet 8
7.2 Informationsöverföring 8
8 Anskaffning, utveckling och avveckling av informationssystem 9
8.1 Anskaffning och utveckling 9
8.2 Avveckling 9
9 Informationssäkerhet avseende verksamhetens kontinuitet 9
10 Efterlevnad 10

Informationssäkerhet, fysisk och teknisk säkerhet – riktlinje

1 Inledning

Information är en av kommunens viktigaste tillgångar och en väsentlig förutsättning för att kunna bedriva verksamheten. Kommunens informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt. Arbetet med informationssäkerhet innefattar flera delar. Utöver införande av administrativa regelverk såsom policys och riktlinjer handlar det även om införande av tekniskt och fysiskt skydd i form av bland annat brandväggar, kryptering, skal- och brandskydd. Informationssäkerhetsarbete handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver.

Informationen ska bevaras utifrån tre informationssäkerhetsaspekter:

- **Konfidentialitet:** att information enbart är tillgänglig för behöriga.
- **Riktighet:** att information är korrekt, aktuell och fullständig.
- **Tillgänglighet:** att information är åtkomlig i rätt tid och användbar av behörig.

Detta dokument vänder sig till de som i Lidköpings 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 det ges i detta dokument hänvisningar till standarden för informationssäkerhet ISO 27000-serien.

2 Avtal med driftsleverantörer

(Ref: ISO 27002: 2022 kap 5.31)

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

Göliska IT är kommunens primära driftsleverantör och delar av kravställningarna avseende fysisk och teknisk säkerhet hanteras i ett kommunövergripande IT-avtal med Göliska IT. Särskilda överenskommelser med anpassat innehåll jämfört med Göliska ITs standardtjänster kan avtalas om separat.

3 Styrning av åtkomst

(Ref: ISO 27002: 2022 kap. 8:1 - 8:3)

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 sektorchef.

3.2 Åtkomst till resurser som hanterar informationstillgångar

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

Endast 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

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

4 Kryptering

(2022 kap 8:24))

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

Bedömning kring behov av kryptering ska baseras på informationens skyddsvärde.

Vid behov av kryptering kan säkerhetsenheten eller Göliska IT kontaktas för lösning. Införande av krypteringslösningar medför krav på rutiner om nyckelhantering, utbildning och resurser.

5 Fysisk och miljörelaterad säkerhet

(Ref: ISO 27002:2022 kap 7)

Informationstillgångar och den utrustning som hanterar dessa 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

5.1 Säkra områden

Systemägaren 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.

Det ska vara dokumenterat vem som har mandat att besluta om besök i utrymmen med särskilt skyddsvärd information eller utrustning.

5.2 Fysiskt skydd för utrustning som hanterar informationstillgångar

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

Rutiner kan omfatta beslut om var utrustning får placeras, tekniska försörjningssystem, kablagesäkerhet, underhåll av utrustning, 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 sektor bildnings IT-team eller Göliska IT beroende på arbetsställe.

Enbart godkänd utrustning får kopplas in i nätverket.

Medarbetares hantering av utrustning framgår av dokumentet Informationssäkerhet för medarbetare och förtroendevalda

6 Driftssäkerhet

(Ref: ISO 27002:2022 kap 8)

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) ska upprättas med alla driftsleverantörer och 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 Utveckling och test

Separata utvecklings- och testmiljöer ska etableras då detta är relevant. Dessa miljöer ska vara skilda från produktionsmiljön.

6.5 Skydd mot skadlig kod

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

Datorer ska vara uppdaterade med senaste säkerhetsuppdateringar. Funktioner för automatiska uppdateringar får inte stängas av.

6.6 Säkerhetskopiering

Systemägaren 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 systemförvaltningsplan. Återställningstester ska genomföras regelbundet.

6.7 Övrigt

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

7 Kommunikationssäkerhet

(Ref: ISO 27002: 2022 kap.5:14, 8:20, 21, 22)

Kommunikationssäkerhet är att säkerställa skyddet av informationstillgångar i nätverk, kringutrustning till nätverk samt utrustning och nätverk som används för datakommunikation.

7.1 Hantering av nätverkssäkerhet

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

(Ref: ISO 27002: 2022, kap 5:20, 21, 22)

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, se Informationssäkerhet vid upphandling - riktlinje.

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. Systemägaren fattar beslut om avveckling. Rutiner för avveckling ska utformas av respektive verksamhet och informationen ska hanteras enligt dokumenthanteringsplan.

9 Informationssäkerhet avseende verksamhetens kontinuitet

(Ref: ISO 27002: 2022 kap.5:30, 8:14)

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.

Driftsleverantören 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

(Ref: ISO 27002: 2022 kap. 5:35)

Granskning av informationssäkerheten ska ske regelbundet för att kontrollera att tillräcklig säkerhetsnivå upprätthålls.

Särskilt viktigt är det att genomföra kontroll och granskning av delar av IT-miljön som direkt eller indirekt stöder system med höga skyddsvärden samt införande av nya IT-lösningar.

Sårbarheter och brister som upptäcks vid granskningar ska tas upp i åtgärdsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till informationsägare och CISO. Rutinen för incident/avvikelserapportering ska följas.