Riktlinje för informationssäkerhet i Linköpings kommun

Dokumenttyp: Riktlinjer
Antaget av: Kommunstyrelsen
Status: Förslag 2019-11-05
Giltighetstid: Gäller tillsvidare

Linköping
Där idéer blir verklighet

Diarienummer:	KS 2018-458
Dokumentansvarig:	Kommundirektör
Adresserat till:	Samtliga nämnder och förvaltningar
Tidpunkt för aktualitetsprövning:	En gång per mandatperiod
Tidpunkt för senaste revidering:	
Relaterade styrdokument:	Informationssäkerhetspolicy, informationssäkerhetshandbok
Sökord:	Informationssäkerhet, infosäk

Innehåll

1 Inledning

Denna riktlinje syftar till att konkretisera informationssäkerhetspolicyn samt ge en vägledning i hur kommunens medarbetare och förtroendevalda ska tillämpa densamma. Det övergripande målet med riktlinjen är att tillse att det operativa informationssäkerhetsarbetet bedrivs i enlighet med vad som föreskrivs nedan samt i övrigt i enlighet med kommunens informationssäkerhetshandbok och gällande lagkrav.

Riktlinjen gäller för alla kommunens nämnder och förvaltningar men inte för dess bolag. Kommunstyrelsen ska, med stöd av denna riktlinje, kunna styra kommunens informationssäkerhetsarbete, i enlighet med MSB:s rekommendationer för kommuners informationssäkerhet samt kraven i informationssäkerhetsstandarden ISO/IEC 27000. Detta görs strategiskt, bland annat genom att ange vad som ska skyddas i kommunens verksamheter samt hur skyddet övergripande ska utformas.

Som stöd i arbetet med att hantera information så att legala, etiska och verksamhetsmässiga intentioner upprätthålls, på det vis som anges i kommunens informationssäkerhetspolicy, ges också kommundirektören i uppdrag att upprätta tillämpningsanvisningar i form av en informationssäkerhetshandbok. Informationssäkerhetshandboken ska utformas i enlighet med informationssäkerhetsstandarden ISO/IEC 27000.

2 Informationssäkerhetsarbete

2.1 Roller, ansvar och befogenheter

Kommunstyrelsen ansvarar för det strategiska arbetet med informationssäkerhet. Med detta menas bland annat att kommunstyrelsen anger vad som ska skyddas, hur en verksamhet ska avgöra lämplig skyddsnivå samt hur det faktiska skyddet uppnås. Detta sker genom antagande av denna riktlinje samt genom att uppdra åt kommundirektören att ta fram därtill hörande tillämpningsanvisningar (informationssäkerhetshandbok). Kommundirektören ansvarar vidare för att tillse att informationssäkerhetshandboken vid behov revideras.

Kommundirektören ansvarar för att organisera informationssäkerhetsarbetet (LIS) i enlighet med informationssäkerhetsstandarden ISO/IEC 27000.

Säkerhetschefen ansvarar för det operativa informationssäkerhetsarbetet i enlighet med vad som anges i informationssäkerhetshandboken.

2.2 Informationsklassning

Informationsklassning ska genomföras för all kommunens information samt därefter tilldelas lämpligt skydd. Samtliga bedömningar av skyddsbehov för information ska göras enligt kommunens modell för informationsklassning.

Modellen består av fem skyddsnivåer vilka framgår av nedanstående tabell (nivå 0-4). Bedömningar av skyddsbehov ska göras utifrån informations-säkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Skydds-nivå	Informationssäkerhetsaspekter			
	Konfidentialitet	**Riktighet**	**Tillgänglighet**	**Spårbarhet**
4 Mycket högt skydds-behov	***Ytterst begränsad*** information, som om den röjs medför *synnerligen allvarlig* konsekvens för kommunen eller annan part t.ex. externa aktörer eller medborgare.	Information som om den inte är riktig och fullständig medför *synnerligen allvarlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför *synnerligen allvarlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför *synnerligen allvarlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
3 Högt skydds-behov	**Strikt begränsad** information, som om den röjs medför *allvarlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information som om den inte är riktig och fullständig medför *allvarlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funk-tion som om den inte är tillgänglig medför *allvarlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför *allvarlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
2 Förhöjt skydds-behov	*Internt begränsad* information, som om den röjs medför *betydande* konse-kvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information som om den inte är riktig och fullständig medför *betydande* konse-kvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funk-tion som om den inte är tillgänglig medför *betydande* konse-kvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför *betydande* konse-kvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
1 Grund-läggande skydds-behov	Intern information, som om den röjs medför *måttlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information som om den inte är riktig och fullständig medför *måttlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför *måttlig* konse-kvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför *måttlig* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
0 Inget skydds-behov	Öppen information som om den röjs medför *ingen, lindrig* eller *försumbar* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information som om den inte är riktig och fullständig medför *ingen, lindrig* eller *försumbar* konse-kvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför *ingen, lindring* eller *försumbar* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför *ingen, lindrig* eller *försumbar* konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.

Tabell 1. Kommunens modell för informationsklassning

2.3 Konsekvenstabell

Kommunens modell för informationsklassning ger uttryck för vilket skyddsbehov en viss information har. Vilket skyddsbehov informationen har avgörs genom att en konsekvensbedömning görs. Detta ska ske genom tillämpning av en konsekvenstabell som ska framgå av informationssäkerhetshandboken. Konsekvenstabellen ska innehålla sex konsekvensområden som relaterar till skyddsnivåerna i klassningsmodellen. Dessa konsekvensområden ska vara:

- Verksamhetens förmåga att utföra sin uppgift
- Ekonomi
- Påverkan på individ
- Påverkan på externa intressenter
- Juridiska aspekter
- Anseende (förtroende/rykte)

För varje konsekvensområde ska eventuella konsekvenser bedömas av att en viss information inte har relevant skydd, i nivåerna 0-3. Nivå 0 ska motsvara lindriga eller försumbara konsekvenser för kommunen, nivå 1 ska motsvara måttliga konsekvenser, nivå 2 betydande konsekvenser och nivå 3 allvarliga konsekvenser.

2.4 Informationssäkerhet för medarbetare med flera

Det operativa arbetet med kommunens informationssäkerhet ska genomföras i alla verksamheter. Samtliga medarbetare och förtroendevalda ska följa riktlinjen och tillhörande informationssäkerhetshandbok. Vissa leverantörer och konsulter ska i berörda delar också följa riktlinjen och tillhörande informationssäkerhetshandbok.

Informationssäkerhetshandboken ska tydliggöra hur ansvaret fördelas samt hur kommunens anställda ska agera när det gäller skydd av information, såväl inom Linköpings kommun som i kontakt med externa parter.

2.5 Informationssäkerhet för informations- och kommunikationsteknologi (ICT)

Den it-tekniska utrustning som lagrar och behandlar information tillhörande Linköpings kommun ska förses med lämpliga skydd för att uppfylla kraven på kommunens informationssäkerhet. Skydden ska omfatta såväl organisatoriska rutiner som tekniska skydd och utformas i enlighet med god säkerhetspraxis.

Informationssäkerhet i den it-nära förvaltningen ska i huvudsak regleras inom följande områden:

- Hantering av tillgångar
- Styrning av åtkomst
- Kryptering
- Fysisk och miljörelaterad säkerhet
- IT-driftsäkerhet

- Kommunikationssäkerhet
- Anskaffning och utveckling av IT-komponenter
- Incidenthantering
- Kontinuitetshantering
- Granskning och kontroll

2.6 Informationssäkerhet i form av fysiskt skydd

Fysiskt skydd av information ska vara en naturlig del i kommunens informationssäkerhetsarbete. Tekniska skydd ska utformas i enlighet med gällande lagstiftning samt följa svenska skyddsnormer och praxis. Fysiskt skydd ska i huvudsak regleras inom följande områden:

- Områdesskydd
- Skalskydd och säkerhetszoner
- Tillträder till utrymmen
- Särskilt skyddsvärda utrymmen (arkiv, datahallar, teleutrymmen etc.)
- Brandskydd
- Skydd av utrustning
- Bevakning
- Fastighetsautomation och övervakning

2.7 Informationssäkerhetsprocesser

För att kunna bedriva kommunens informationssäkerhetsarbete med kontinuitet och bibehållen kvalitet ska ett antal verksamhetsprocesser inom informationssäkerhet upprättas i verksamheten. Dessa processer ska anpassas till Linköpings kommuns verksamhet och utformas i enlighet med tillämpliga delar i informationssäkerhetsstandarden ISO/IEC 27000.

Följande processer med tillhörande anvisningar ska skapas för verksamheterna i den verksamhetsnära förvaltningen, utifrån beskrivning i informations-säkerhetshandboken:

- **Informationsklassningsprocess** för identifiering och tilldelning av lämpliga skyddsbehov ska tillämpas.
- **Riskhanteringsprocess** för identifiering och hantering av informationssäkerhetsrelaterade risker ska tas fram och tillämpas.

- **Incidenthanteringsprocess** där anvisningar ska beskriva processen för hantering och uppföljning av informationssäkerhetsrelaterade incidenter ska tas fram och tillämpas.

- **Behörighetshanteringsprocess** för arbete med tilldelning, upprätthållande och avveckling av behörigheter till kommunens information ska tas fram och tillämpas.

- **Personalsäkerhetsprocess** för informationssäkerhetsrelaterade moment innan anställning, under anställning och vid anställningens upphörande ska tas fram och tillämpas.

- **Process för anskaffning, utveckling och avveckling av tjänster/system** avseende informationssäkerhetsrelaterade moment i arbetet med anskaffning, utveckling och avveckling av tjänster och system ska tas fram och tillämpas.

- **Kontinuitetsplaneringsprocess** för hur tillgång till kommunens information ska kravställas och optimeras utifrån de verksamheternas behov ska tas fram och tillämpas.

- **Säkerhetsmedvetandeprocess** för hur medvetenhet kan vidimeras och hur medvetenhet ska förmedlas ska tas fram och tillämpas.

- **Uppföljning och efterlevnadsprocess** för uppföljning av informationssäker hetsarbetet i verksamheten samt hur regleringar inom området ska efterlevas förmedlas ska tas fram och tillämpas.

- **Ledningsprocess** för hur ledningen ska styra informationssäkerhetsarbetet och hur ledningen återkopplar arbetet till verksamheten ska tas fram och tillämpas.