ör
nssäkerhet

I Linköpings kommun

Dokumenttyp: Riktlinje
Antaget av: Kommunstyrelsen 2019-11-19, § 359Senast reviderat:
Kommunstyrelsen 2021-04-20, § x
Giltighetstid: Gäller tills vidare

Diarienummer: KS 2018-458

Dokumentansvarig: Kommundirektören

Adresserat till: Samtliga nämnder

Tidpunkt för aktualitetsprövning:

Relaterade styrdokument: Säkerhetspolicy, Informationssäkerhetshandbok

Sökord: LIS, Informationssäkerhet, Info Säk

Innehåll

1 Inledning 4

2 Informationssäkerhetsarbete 4

2.1 Ansvar och befogenheter 4
2.2 Informationssäkerhetshandbok 4
2.3 Informationsklassning 5
2.4 Konsekvenstabell 7
2.5 Informationssäkerhet för medarbetare med flera 7
2.6 Informationssäkerhet för informations- och kommunikationsteknologi (ICT) 7
2.7 Informationssäkerhet i form av fysiskt skydd 8
2.8 Informationssäkerhetsprocesser 8

1 Inledning

Denna riktlinje syftar till att konkretisera säkerhetspolicyn vad avser informationssäkerhetsarbetet i kommunen. Det övergripande målet med riktlinjen är att tillse att det operativa informationssäkerhetsarbetet bedrivs i enlighet med gällande lagstiftning.

Riktlinjen gäller för alla kommunens nämnder och förvaltningar. Kommunstyrelsen ska, med stöd av denna riktlinje, kunna styra kommunens informationssäkerhetsarbete, i enlighet med MSB:s rekommendationer för kommuners informationssäkerhet samt med beaktande av kraven i informationssäkerhetsstandarden ISO/IEC 27000, där så anges i tillämpningsanvisningarna. Detta görs strategiskt, bland annat genom att, i tillämpningsanvisningar, 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 säkerhetspolicy, har kommundirektören därför uppdraget att upprätta och vid behov revidera tillämpningsanvisningar i form av en informationssäkerhetshandbok.

2 Informationssäkerhetsarbete

2.1 Ansvar och befogenheter

Kommunstyrelsen ansvarar, i enlighet med säkerhetspolicyn, 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. Kommundirektören har i uppdrag att ta fram tillämpningsanvisningar, bl.a. i form av en informationssäkerhetshandbok.

Förändringar i informationssäkerhetshandboken som är av principiell beskaffenhet eller annars av större vikt, såsom sådant som påverkar kommunens risker, konsekvensbedömningar, antal skyddsnivåer eller andra grundläggande strukturer i informationssäkerhetsarbetet ska beslutas av kommunstyrelsen.

2.2 Informationssäkerhetshandbok

Kommundirektören har i uppdrag att ta fram tillämpningsanvisningar, bl.a. i form av en informationssäkerhetshandbok. Uppdraget innefattar även att vid behov tillse att tillämpningsanvisningarna revideras.

Informationssäkerhetshandboken och eventuellt övriga till området hörande tillämpningsanvisningar och rutiner ska, utifrån säkerhetspolicyn tydliggöra och konkretisera denna riktlinje. Detta innefattar bl.a. reglering av hur ansvaret ska fördelas samt hur kommunens anställda ska agera när det gäller skydd av information, såväl inom kommunen som i kontakt med externa parter. Det

innefattar även reglering av hur det faktiska informationssäkerhetsarbetet ska genomföras i kommunens verksamheter.

Informationssäkerhetshandboken reglerar inte hanteringen av säkerhetsskyddsklassificerade uppgifter, det vill säga informationssäkerhetsklass 4. Dessa uppgifter regleras i andra styrdokument.

2.3 Informationsklassning

Informationsklassning ska genomföras för all kommunens information för att därefter kunna tilldela informationen 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 informationssäkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Skyddsnivå	Säkerhetsaspekter			
	Konfidentialitet	**Riktighet**	**Tillgänglighet**	**Spårbarhet**
4 **Säkerhets-skydds-klassificerade uppgifter** Mycket högt skyddsbehov	Säkerhetsskydds-klassificerade uppgifter. Information som rör Sveriges säkerhet.	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 **Stark sekretess** Högt skyddsbehov	Information som innehåller uppgift som omfattas av stark eller absolut sekretess eller uppgift som hänför sig till 18 kap OSL, eller en mycket stor mängd känsliga personuppgifter som inte omfattas av stark eller absolut sekretess, där felaktig spridning kan medföra allvarliga konsekvenser för kommunen eller annan part.	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 funktion 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 **Sekretess** Förhöjt skyddsbehov	Information som omfattas av svag sekretess enligt OSL eller känsliga personuppgifter enligt GDPR, där spridning kan medföra betydande konsekvenser för kommunen eller annan part.	Information som om den inte är riktig och fullständig medför betydande konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför betydande konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför betydande konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
1 **Intern information** Grundläggande skyddsbehov	Information som är avsedd att spridas fritt enbart till medarbetare inom Linköpings kommun och till externa aktörer som behöver informationen.	Information som om den inte är riktig och fullständig medför måttligt negativ konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför måttligt negativ konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför måttligt negativ konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
0 **Öppen information** Inget skyddsbehov	Öppen information som är avsedd att spridas fritt inom och utom Linköpings kommun.	Information som om den inte är riktig och fullständig medför lindrig eller försumbar negativ konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför lindring eller försumbar negativ konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför lindrig eller försumbar negativ konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.

2.4 Konsekvenstabell

Kommunens modell för informationsklassning ska alltså visa vilket skyddsbehov en viss information har. För säkerhetsaspekten konfidentialitet gäller en direkt koppling till gällande lagstiftning avseende offentlighet och sekretess samt dataskyddsförordningen. För övriga säkerhetsaspekter gäller att skyddsbehovet för informationen avgörs genom att nedanstående konsekvenstabell tillämpas. Konsekvenstabellen innehåller sex konsekvensområden som relaterar till skyddsnivåerna i klassningsmodellen. Dessa konsekvensområden är:

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

För varje konsekvensområde bedöms eventuella konsekvenser av att en viss information inte har relevant skydd, i nivåerna 0-3, där 0 motsvarar lindriga eller försumbara konsekvenser för kommunen, 1 motsvarar måttliga konsekvenser, 2 betydande konsekvenser och 3 allvarliga konsekvenser. Vid informationsklassning ska alltså verksamheten, utifrån den konsekvenstabell som framgår av informationssäkerhetshandboken, bedöma skyddsbehovet av en viss information, genom att analysera och värdera konsekvenserna av att informationen ifråga sprids.

2.5 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.

2.6 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
- Leverantörsstyrning
- Styrning av åtkomst
- Kryptering
- Fysisk och miljörelaterad säkerhet
- It-driftsäkerhet

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

2.7 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
- tillträde till utrymmen
- särskilt skyddsvärda utrymmen (arkiv, datahallar, teleutrymmen etc.)
- brandskydd
- skydd av utrustning
- bevakning
- fastighetsautomation och övervakning

2.8 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.

Mot bakgrund av ovanstående ska följande processer med tillhörande anvisningar, vilka närmare regleras i informationssäkerhetshandboken, skapas för och tillämpas av verksamheterna i den verksamhetsnära förvaltningen:

- **Informationsklassningsprocess** för identifiering och tilldelning av lämpliga skyddsbehov.

- **Riskhanteringsprocess** för identifiering och hantering av informationssäkerhetsrelaterade risker.

- **Incidenthanteringsprocess** som reglerar hantering och uppföljning av informationssäkerhetsrelaterade incidenter.

- **Behörighetshanteringsprocess** som reglerar arbetet med tilldelning, upprätthållande och avveckling av behörigheter till kommunens information.

- **Personalsäkerhetsprocess** för informationssäkerhetsrelaterade moment innan anställning, under anställning och vid anställningens upphörande.

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

- **Kontinuitetsplaneringsprocess** som reglerar hur tillgång till kommunens information ska kravställas och optimeras utifrån verksamheternas behov.

- **Säkerhetsmedvetandeprocess** som anger hur medvetenheten om informationssäkerhet ska förmedlas och vidmakthållas.

- **Uppföljningsprocess** som anger hur uppföljning av informationssäkerhetsarbetet ska ske i verksamheten samt hur efterlevnaden ska säkerställas.

- **Ledningsprocess** som reglerar hur styrningen av informationssäkerhetsarbetet ska ledas och återkopplas till verksamheten.