LJUNGBY
KOMMUN

Diarienummer: KS 2018/0362.016.

Verksamhetsplan

Informationssäkerhet

Gäller från:	2018-12-04
Gäller för:	Hela kommunkoncernen
Globalt mål:	
Fastställd av:	Kommunstyrelsen
Utarbetad av:	Annika Sandström
Revideras senast:	2022-12-31
Version:	2
Dokumentansvarig förvaltning:	Kommunledningsförvaltningen

Ett utskrivet dokument är alltid en kopia, giltig version finns alltid på intranätet.

LJUNGBY
KOMMUN

Innehållsförteckning

Inledning

Denna verksamhetsplan gäller för Ljungby kommun inklusive de helägda kommunala bolagen.

Information är en av kommunens och bolagens viktigaste tillgångar och vårt ansvar spänner över ett stort område av samhällsviktig verksamhet. I samtliga delar spelar en säker informationshantering en central roll. Med information avses all information, oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i. Information återfinns även som den samlade kunskapen hos kommunens medarbetare. Informationssäkerhet är det samlade arbetet som görs för att hålla kommunens information säker med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Informationssäkerhetsarbetet bygger på standarden ISO/IEC 27001.

Syfte

Verksamhetsplan för informationssäkerhet beskriver kommunens mål och organisation för informationssäkerhetsarbetet. Verksamhetsplanen följer Policy för trygghet och säkerhet (KS2016/0245.016).

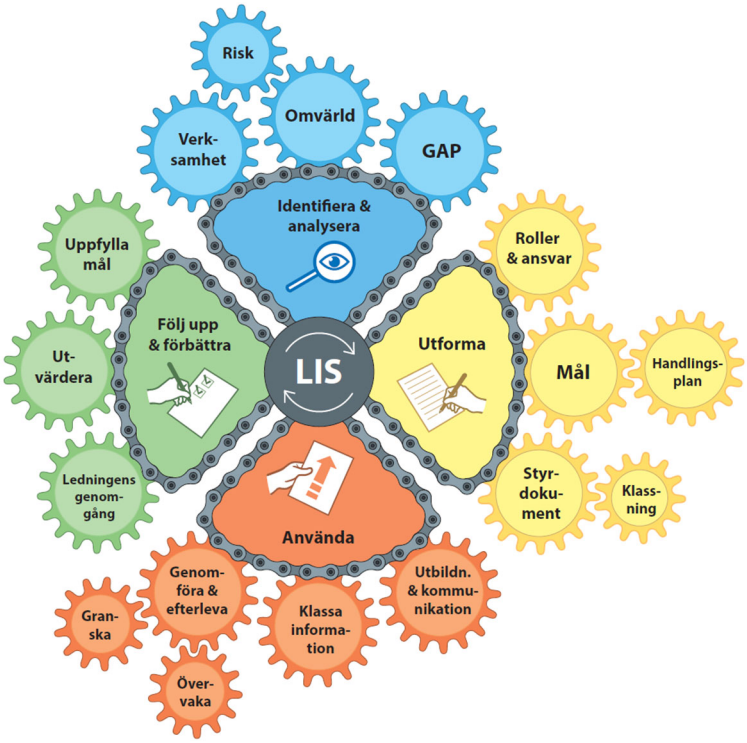
Omfattning

Verksamhetsplan för informationssäkerhet och relaterade dokument och riktlinjer omfattar kommunens information och alla som kommer eller kan komma i kontakt med kommunens information. Detta gäller utan undantag.

Mål

- Att det systematiska informationssäkerhetsarbetet utformas och följer principerna för LIS - ledningssystem för informationssäkerhet.

Ledningssystem för informationssäkerhet är ett stöd för systematiskt arbete med informationssäkerhet i organisationer. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna i organisationen, som planering och uppföljning. Ledningssystemet bygger därmed på organisationens planerings- och uppföljningscykler. Dessa cykler innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och -kontroller samt ser över styrdokumenten med jämna mellanrum.



Definition av informationssäkerhet

Informationssäkerhet innebär att på ett systematiskt sätt och efter behov skydda informationen vi hanterar. Värdefull information måste skyddas så att

- endast behöriga personer får ta del av den (konfidentialitet).
- vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet).
- den alltid finns när vi behöver den (tillgänglighet).
- det går att följa vem som har tagit del av information, vilka förändringar som har gjorts och av vem (spårbarhet).

LJUNGBY
KOMMUN

Omvärldsanalys - Lagar och regelverk

Externa krav i form av lagar och regelverk har betydelse för kommunens informationshantering. Alla verksamheter berörs i någon omfattning av dessa.

Rättsligt skydd för viss typ av information

Vissa särskilda typer av information skyddas på olika sätt genom bestämmelser i olika lagar.

Allmänna handlingar: Tryckfrihetsförordning, Offentlighets- och sekretesslag.
Sekretessbelagd information rörande Sveriges säkerhet: Säkerhetsskyddslag, Säkerhetsskyddsförordning, Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd.
Personuppgifter: Dataskyddsförordningen (GDPR).
Information som ska arkiveras: Arkivlag, Arkivförordning, Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar, Riksarkivets föreskrifter om och allmänna råd om tekniska krav på elektroniska handlingar.

Rättsliga krav på informationssäkerhet i olika verksamheter

Samhällsviktiga tjänster

EU:s NIS-direktiv[i] ställer krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster[ii] och vissa digitala tjänster. För Ljungby kommun och de kommunala bolagen är direktivet tillämpligt inom sektorerna energi, hälso- och sjukvård samt leverans och distribution av dricksvatten. Direktivet införlivas i den svenska rättsordningen genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174) och regeringen har beslutat om en förordning (2018:1175) kopplat till den nya lagen. Lagen och förordningen träder i kraft 1 augusti 2018.

Hälso- och sjukvård

Inom hälso- och sjukvården hanteras stora mängder ur integritetssynpunkt känslig information. Det är av stor vikt att informationshanteringen inom hälso- och sjukvården är organiserad så att den tillgodoser patientsäkerhet och god kvalitet och kostnadseffektivitet. Att säkerställa respekt för patienters och övriga registrerades integritet är prioriterat liksom arbetet med att säkerställa att inga obehöriga får tillgång till dokumenterade personuppgifter. Patientdatalag, Patientdataförordning samt socialstyrelsens föreskrifter reglerar området.

IT-brott och IT-relaterad brottslighet

Dataintrång

Enligt brottsbalken 4 kap 9c§ är det förbjudet att olovligen bereda sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändra, utplåna, blockera eller i register föra in en sådan uppgift. Det är heller inte tillåtet att olovligen allvarligt störa eller hindra användningen av en sådan uppgift. Ett nytt brott, grovt dataintrång, infördes i brottsbalken 2014. Ett dataintrång ska bedömas som grovt om det har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit särskilt farlig.

Interna krav – reglementen och ägardirektiv

Kommunallagen (1991:900), KL, ger de grundläggande reglerna för ansvar och beslutanderätt i en kommun. Utöver kommunallagen gäller bestämmelser i styrelsens och nämndernas reglementen, som beslutas av kommunfullmäktige. I reglementena preciseras nämndernas verksamhet och ansvarsområden. För bolagen gäller ägardirektiv fastställda av kommunfullmäktige.

Roller, ansvar och organisation

Grundprincipen är att ansvaret för själva informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret. Detta gäller från politisk ledning till enskilda medarbetare. Informationssäkerhetsarbetet ska alltså vara integrerat i ordinarie arbete enligt modellen för LIS.

Kommunfullmäktige fastställer policy för trygghet och säkerhet.

Kommunstyrelsen beslutar om verksamhetsplan för informationssäkerhet. KS är därtill liksom **övriga nämnder och styrelser** ansvarig för informationssäkerheten inom sitt verksamhetsområde. Nämnder och styrelser ska löpande följa upp informationssäkerhetsarbetet och vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Kommundirektör och övriga förvaltningschefer samt VD:ar ansvarar operativt över verksamhetens systematiska informationssäkerhetsarbete och dess styrning för att säkerställa dess fortsatta lämplighet, tillräcklighet och verkan. De tar beslut om arbetets inriktning och resurser.

Säkerhetsskyddschefen leder och samordnar arbetet med informationssäkerhet kopplat till rikets (Sveriges) säkerhet det vill säga säkerhetsskyddsklassificerade uppgifter.

Funktionen som arbetar med informationssäkerhet (informationssäkerhetssamordnaren) ansvarar för att leda och samordna informationssäkerhetsarbetet genom att kontinuerligt planera, genomföra, kontrollera, följa upp, utvärdera och förbättra.

Systemförvaltarorganisationen ansvarar för systemförvaltningen enligt systemägarens instruktioner (systemförvaltningsplan). De ansvarar därmed för att identifiera behov och ställa krav gällande informationssäkerhet för respektive system.

Arbetsgrupp för trygghet och säkerhet är kommunens förvaltningsövergripande forum för frågor som rör trygghet och säkerhet. Gruppen utgör referensgrupp för informationssäkerhetsarbetet.

För att kunna upprätthålla en god informationssäkerhet och förankra detta i organisationen ska det finnas resurser för ett systematiskt arbete.

Uppföljning och revidering

Verksamhetsplan för informationssäkerhet ska revideras en gång per mandatperiod, eller behovsprövat vid till exempel förändrad lagstiftning eller interna krav.

Verksamhetsplanen konkretiseras i form av en handlingsplan, där det övergripande målet bryts ner till en planering för mandatperioden. Åtgärderna i handlingsplanen ska följas upp en gång per år och presenteras i den förvaltningsövergripande ledningsgruppen.

[i] I juli 2016 antog Europaparlamentet det så kallade NIS-direktivet med åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen. Läs mer här: https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/

[ii] Samhällsviktiga tjänster delas in i sju sektorer; energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, leverans och distribution av dricksvatten och digital infrastruktur.