

A large, abstract blue shape that resembles a stylized letter 'P' or a curved arrow pointing to the right, occupying the left and center of the page.

Riktlinje för informationssäkerhet

Policy

Strategi

▶ Riktlinje

Plan

Beslutad av:	Diarienummer:	Typ av styrdokument:	Dokumentansvarig:
Kommunstyrelsen	2026-000099	Riktlinje	Kanslienheten
Beslutsdatum och paragraf:	Giltig till:	Senast reviderad:	
2026-03-10 § 64	Tills vidare	2026-03-10	

Innehåll

1. Inledning.....	3
2. Syfte och mål.....	3
3. Avgränsning	4
4. Definition av informationssäkerhet.....	4
5. Definitioner	4
6. Regelverk	6
Kommande regelverk	6
7. Roller och ansvar.....	7
Kommunstyrelsen.....	7
Nämnder	7
Kommunchef.....	8
Förvaltningschef.....	8
Informationssäkerhetssamordnare.....	8
IT-säkerhetsansvarig	9
Dataskyddsombud	9
Medarbetare.....	9
Säkerhetsskyddschef	10
8. Systemförvaltning	10
Systemägare	10
Systemförvaltare.....	10
9. Informationssäkerhetskultur.....	10
10. Utbildning.....	11
11. Informationsklassning	11
12. Riskhantering	12
13. Upphandling	12
Informationssäkerhet och dataskydd (GDPR) vid upphandling.	13
14. Incidenthantering.....	13
15. Fysiskt skydd.....	14
16. Uppföljning och förbättring	15

1. Inledning

Riktlinjen utgår från Laholms kommuns policy för informationssäkerhet (dnr KS 2025–000422) och beskriver hur informationssäkerhetsarbetet ska bedrivas inom samtliga nämnder och kommunägda bolagen. Riktlinjen är bindande och det finns inte utrymme för lokala avvikelser.

Informationssäkerhet är en förutsättning för att Laholms kommun ska kunna fullgöra sina uppdrag på ett tryggt, effektivt och rättssäkert sätt. Arbetet ska bidra till att minimera risken för störningar, stärka kommunens motståndskraft och säkerställa förmågan till återhämtning vid incidenter.

Riktlinjen gäller all information som hanteras inom Laholms kommun, oavsett form (digital, fysisk, muntlig) eller lagringsyta. All information ska skyddas utifrån principerna *konfidentialitet, riktighet* och *tillgänglighet*.

Som ett komplement till dessa principer lyfts även *spårbarhet* fram som en viktig förutsättning för att säkerställa riktighet och ansvar. Genom att kunna följa vem som har hanterat informationen, när och hur, stärks både kvaliteten i informationshanteringen och möjligheten att upptäcka och åtgärda fel eller avvikelser.

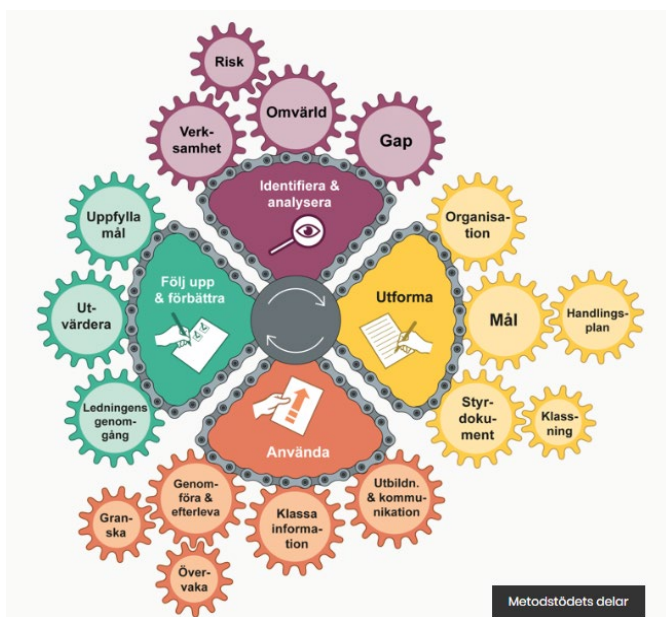
Denna riktlinje ersätter Riktlinje Informationssäkerhet (dnr KS 2021–000166).

2. Syfte och mål

Syftet med denna riktlinje är att skapa ett långsiktigt informationssäkerhetsarbete inom Laholms kommun. Arbetet ska skydda informationstillgångar, hantera olika risker och säkerställa att lagar och interna krav följs.

Ett centralt mål är att införa och vidareutveckla ett ledningssystem för informationssäkerhet (LIS) som bygger på den internationella standarden ISO/IEC 27001. Arbetet utgår från MCF - Myndigheten för civilt försvars, (*tidigare MSB*), metodstöd för systematiskt informationssäkerhetsarbete, vilket ger en tydlig struktur för att upprätta, införa, driva, underhålla och kontinuerligt förbättra informationssäkerhetsarbetet.

Metodstödet bygger på principen om ständig förbättring (Plan-Do-Check-Act), vilket säkerställer att informationssäkerheten följs upp och utvecklas systematiskt över tid.



Bildkälla: MCF (Myndigheten för civilt försvar)

3. Avgränsning

Denna riktlinje omfattar inte säkerhetsskyddsklassificerade uppgifter eller frågor som regleras i säkerhetsskyddslagsstiftningen. Dessa hanteras i en särskild rutin: "Rutin för behandling av säkerhetsskyddsklassificerade uppgifter" (dnr KS 2023–000379).

Frågor som rör behandling av personuppgifter omfattas inte av denna riktlinje utan regleras i "Riktlinje för behandling av personuppgifter i Laholms kommun" (dnr KS 2018–000038).

4. Definition av informationssäkerhet

Informationssäkerhet innebär att på ett systematiskt sätt skydda informationen vi hanterar. Informationen behöver skyddas så att:

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

5. Definitioner

Begrepp	Definition
<i>Behörighet</i>	Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.
<i>Betydande incident</i>	En händelse som orsakar eller riskerar att orsaka allvarliga störningar i en verksamhet eller dess nätverks- och informationssystem.
<i>Cybersäkerhet</i>	Skyddande av digitala system och nätverk från elektroniska hot och obehörig åtkomst.
<i>Incidentrapportering</i>	En process för att anmäla och beskriva en informationssäkerhetsincident.
<i>Informationsklassning</i>	En process där man värderar information utifrån vilka konsekvenser ett otillräckligt skydd skulle få.
<i>Informationssystem</i>	En kombination av människor, processer och teknik som hanterar information för att stödja verksamheten.
<i>Informationssäkerhetsincident</i>	En händelse som påverkar eller hotar informationssäkerheten i en organisation. Detta kan inkludera förlust, stöld, obehörig åtkomst, skadlig programvara, IT-avbrott och oavsiktlig exponering, orsakade av mänskliga faktorer, naturhändelser, hotaktörer eller systemändringar.
<i>Informationssäkerhetsrisk</i>	En kombination av sannolikhet och konsekvens. Sannolikheten att en viss händelse inträffar i nätverks- och informationssystem och dess potentiella konsekvenser.
<i>Informationstillgång</i>	Innefattar både den information, och de informationssystem som hanterar informationen, som är av värde för en organisation.
<i>Informationsägare</i>	Roll som innebär ett utpekat ansvar för information inom ett eller flera verksamhetsområden och hanteras inom den egna verksamheten.
<i>Kontinuitet</i>	Säkerställande att verksamheten kan fortsätta bedrivas vid allvarlig störning eller avbrott.
<i>Ledningssystem för informationssäkerhet (LIS)</i>	Del av organisationens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla

	och förbättra organisationens informationssäkerhet.
Personuppgiftsincident	Är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, obehörigt röjande/åtkomst eller ändring av personuppgifter.
Riskhantering	Samordnade aktiviteter för att styra och leda en organisation med avseende på risk.
Systemägare	Roll som har ett överordnat ansvar för administration, drift och säkerhet för ett informationssystem.

6. Regelverk

Informationssäkerhetsarbetet inom Laholms kommun ska bedrivas i enlighet med gällande lagstiftning, föreskrifter och kommunens egna styrdokument. Det innebär att arbetet ska ta hänsyn till bland annat:

- ❖ **Allmänna handlingar** – Tryckfrihetsförordningen, Offentlighets- och sekretesslag.
- ❖ **Sekretessbelagd information rörande Sveriges säkerhet** – Säkerhetsskyddslag, Säkerhetsskyddsförordning, Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd.
- ❖ **Personuppgifter** – Dataskyddsförordningen (GDPR), Dataskyddslagen.
- ❖ **Information som ska arkiveras** – Arkivlag, Arkivförordning samt Laholms Riktlinje för hantering av arkiv.
- ❖ **Hälso- och sjukvård** – Patientdatalag, Patientdataförordningen, samt Socialstyrelsens föreskrifter.
- ❖ **NIS2-direktivet**
 - Gäller i EU sedan 2023 och syftar till att höja den gemensamma säkerhetsnivån inom medlemsländerna. Direktivet ställer högre krav på riskhantering, kontroll av leverantörer, incidentrapportering och säkerhetsåtgärder för samhällsviktiga och digitala tjänster.
 - **Cybersäkerhetslagen**
Cybersäkerhetslagen är den svenska implementeringen av NIS2 och omfattar olika sektorer som offentlig förvaltning som samhällsviktiga aktörer. Detta innebär att hela Laholms kommuns verksamheter omfattas av lagens krav.
- ❖ **AI-act** - Antagen av EU 2024.
Förordningen reglerar utveckling, användning och inköp av AI-system och inför krav baserade på risknivåer. Kommuner som använder eller upphandlar AI-tjänster kommer omfattas av krav på riskbedömning, transparens, dokumentation och leverantörskontroll. Tillämpas stegvis under 2025–2026.

Kommande regelverk

Laholms kommun ska även bevaka och förbereda sig för kommande regelverk som påverkar informationssäkerhetsarbetet:

❖ CER-direktivet (Critical Entities Resilience)

- Trädde i kraft i EU 2023. Direktivet syftar till att stärka motståndskraften hos samhällsviktiga aktörer mot fysiska hot, störningar och kriser och harmoniserar med NIS2-direktivet som fokuserar på cybersäkerhet. Tillsammans utgör de en helhetssyn på säkerhet och kontinuitet för samhällsviktiga funktioner. En svensk lag om kritiska entiteters motståndskraft är under utredning och förväntas träda i kraft någon gång under 2026. Kommuner som bedriver samhällsviktig verksamhet som exempelvis hälso- och sjukvård, utbildning och infrastruktur kommer omfattas. Laholms kommun ska därför bevaka utvecklingen och förbereda sig för att uppfylla kommande krav på fysisk säkerhet, kontinuitet och krisberedskap.

7. Roller och ansvar

Ansvar för informationssäkerheten följer ordinarie verksamhetsansvar. Detta gäller från kommunstyrelsen till den enskilde medarbetaren. Alla i Laholms kommun och de kommunala bolagen är utifrån sitt eget uppdrag ansvarig för sin del av informationssäkerheten.

I detta avsnitt beskrivs de övergripande rollerna och deras ansvar i informationssäkerhetsarbetet. I de efterföljande avsnitten förtydligas ansvaret inom respektive område.

Kommunstyrelsen

Kommunstyrelsen har ett övergripande ansvar för att informationssäkerhetsarbetet bedrivs i linje med den fastställda policyn för informationssäkerhet och koordinerar arbetet med informationssäkerhet och verkar normerande, stödjande och uppföljande i relation till Laholms kommuns samtliga verksamheter.

Kommunstyrelsen har utifrån sin roll även ett ansvar att säkerställa att ledningen genomgår utbildning i informationssäkerhet och cybersäkerhet, i enlighet med krav i den nya cybersäkerhetslagen.

Nämnder

Varje nämnd är informationsägare och har det yttersta ansvaret för den information som hanteras inom den egna förvaltningen. Detta ansvar innefattar att:

- genomgå grundläggande utbildning i informationssäkerhet för att kunna fatta välgrundade beslut.
- följa upp att informationssäkerhetsarbetet bedrivs i enlighet med Laholms kommuns policy, riktlinje och regelverk inom den egna förvaltningen, regelbundet och minst årligen, samt vid behov.
- vidta nödvändiga åtgärder för att uppnå och upprätthålla en god informationssäkerhet.
- säkerställa att förvaltningen har rutiner för informationsklassning, riskhantering och incidentrapportering.
- säkerställa att informationssäkerhetsincidenter inom den egna verksamheten rapporteras, hanteras och följs upp.

- säkerställa att det finns en informationssäkerhetsansvarig inom sitt område.
- säkerställa att samtliga system i den digitala miljön har en systemägare inom förvaltningens ansvarsområde.

Kommunchef

Kommunchefen ansvarar för att leda och samordna det kommunövergripande informationssäkerhetsarbetet samt säkerställa att förvaltningscheferna följer fastställda styrdokument.

Förvaltningschef

Förvaltningschefen ansvarar för att omsätta nämndens informationssäkerhetsansvar i praktisk styrning och ledning i verksamheten. Det innebär att:

- säkerställa att informationsklassning, riskhantering och uppföljning genomförs inom förvaltningen.
- utse ansvariga roller inom förvaltningen, exempelvis systemägare, systemförvaltare och förvaltningens representant till informationssäkerhetsnätverk.
- stödja medarbetare i att följa säkerhetsrutiner och främja en god säkerhetskultur.
- genomgå obligatorisk utbildning i informationssäkerhet.
- säkerställa att det finns rutiner för att upptäcka, rapportera och hantera informationssäkerhetsincidenter.
- säkerställa att fysisk informationssäkerhet beaktas i lokaler, utrustning och arbetsmiljö.
- utse och säkerställa att systemägarnas ansvar är dokumenterat och efterlevs.
- säkerställa att chefer inom förvaltningen följer systemförvaltarplanen för att meddela förändringar i anställning eller uppdrag som påverkar systembehörigheter.

I kommunala bolag har VD motsvarande ansvar som förvaltningschef i kommunens förvaltningar.

Informationssäkerhetssamordnare

Informationssäkerhetssamordnaren har ett samordnande och stödjande ansvar för att utveckla och införa ett ledningssystem för informationssäkerhet (LIS) inom Laholms kommun. Rollen innefattar att:

- driva det systematiska informationssäkerhetsarbetet i enlighet med ISO/IEC 27001 och MCF:s metodstöd.
- samordna, följa upp och utveckla Laholms kommuns ledningssystem för informationssäkerhet (LIS).
- ge stöd till verksamheter och nämnder i deras informationssäkerhetsarbete.
- samordna riskanalyser, utbildningsinsatser och uppföljningar.
- ta fram och förvalta styrande dokument inom området.
- vara sammankallande av informationssäkerhetsnätverk.
- ge stöd vid hantering och analys av informationssäkerhetsincidenter samt rapportera betydande incidenter till berörd myndighet.

IT-säkerhetsansvarig

IT-säkerhetsansvarig har ett tekniskt och operativt ansvar för att säkerställa att Laholms kommuns IT-miljö är säker, robust och i linje med gällande krav. Rollen innefattar att:

- säkerställa att tekniska säkerhetsåtgärder (brandväggar, antivirus, behörighetsstyrning, loggning, backup) är korrekt implementerade och uppdaterade.
- samverka med informationssäkerhetssamordnaren och systemägare för att säkerställa att tekniska lösningar möter verksamhetens behov och säkerhetskrav.
- delta i riskanalyser, informationsklassningar, och bidra med teknisk kompetens vid bedömning av säkerhetsrisker.
- övervaka och hantera säkerhetsincidenter i IT-miljön, inklusive rapportering och återställning.
- följa utvecklingen inom cybersäkerhet och föreslå förbättringar av tekniska säkerhetslösningar.
- samverka med fastighetsansvariga för att säkerställa att teknisk utrustning (servrar, nätverk) är fysiskt skyddad.

Dataskyddsombud

Dataskyddsombudet övervakar att Laholms kommun följer dataskyddsförordningen och dataskyddslagen.

Se Riktlinje för behandling av personuppgifter i Laholms kommun (dnr KS 2018–000038).

Medarbetare

Alla medarbetare i Laholms kommun och de kommunala bolagen har ett ansvar att bidra till en säker informationshantering i sitt dagliga arbete. Det innebär att varje medarbetare ska:

- följa Laholms kommuns policy- och riktlinje för informationssäkerhet.
- hantera information enligt gällande regler för sekretess.
- rapportera misstänkta säkerhetsincidenter, avvikelser eller IT-problem via kommunens utsedda kanaler för incidentrapportering.
- delta i utbildningar om informationssäkerhet.
- vara uppmärksam på risker i den digitala arbetsmiljön. Exempelvis nätfiske, otillåten åtkomst eller hanteringen av lösenord.
- vara uppmärksam på risker i den fysiska arbetsmiljön. Exempelvis att låsa datorer och andra inloggade enheter när de lämnas obevakade samt att inte släppa in overifierade personer i Laholms kommuns lokaler.
- hantera fysisk information (utskrifter, anteckningar, USB-minnen) på ett säkert sätt och skydda den från obehörig åtkomst.
- bidra till en god informationssäkerhetskultur genom att hantera information på ett ansvarsfullt sätt i tjänsten.

Medarbetare bör även vara medvetna om att information som rör kommunen kan spridas även utanför arbetet, och därför vara försiktiga med att dela arbetsrelaterad information i privata sammanhang.

Säkerhetsskyddschef

Säkerhetsskyddschefen ansvarar för att samordna säkerhetsskyddsarbetet i enlighet med säkerhetsskyddslagen. Rollen är separat från det generella informationssäkerhetsarbetet, men ska samverka med informationssäkerhetssamordnaren vid behov. Säkerhetsskyddschefen ansvarar för säkerhetsanalys, skydd av säkerhetsklassad information, säkerhetsprovning och rapportering av incidenter till Säkerhetspolisen.

8. Systemförvaltning

Systemförvaltning omfattar ansvar för att säkerställa att Laholms kommuns IT-system och digitala tjänster uppfyller krav på tillgänglighet, säkerhet, funktionalitet och efterlevnad. Roller inom systemförvaltning ska samverka med informationssäkerhetssamordnare, IT-säkerhetsansvarig och verksamhetsansvariga.

Systemägare

I systemägarens ansvar ska det ingå att säkerställa att informationssäkerhetskrav beaktas i systemets hela livscykel, inklusive behörighetsstyrning, riskhantering och uppföljning.

Systemförvaltare

Systemförvaltaren ansvarar för att samordna systemets användning och säkerställa att informationssäkerhetskrav omsätts i praktiken. Systemförvaltaren deltar i riskanalyser, följer upp behörigheter och rapporterar incidenter.

Detaljerade ansvarsområden finns i Anvisning för Systemförvaltning (dnr KS 2018–000240).

9. Informationssäkerhetskultur

Informationssäkerhetskultur handlar om en organisations gemensamma sätt att tänka, agera och förhålla sig till risk och säkerhet. Det innebär hur en organisation prioriterar, kommunicerar och arbetar med risker och säkerhet kopplat till sin verksamhet.

En stark informationssäkerhetskultur bidrar till att säkerhet blir en naturlig del av vardagen. Alla medarbetare ska känna ansvar för att skydda information och därmed bidra till en trygg digital och fysisk arbetsplats.

Det är viktigt att Laholms kommun har en rättvis och rapportrande kultur kring informationssäkerhetsfrågor. Det menas med att medarbetare ska uppmuntras, vågas och ska veta hur de ska rapportera olika fel, brister, incidenter och misstag utan rädsla för skuld eller bestraffning. Informationssäkerhetskultur bygger på tillit, tydliga rutiner och kommunikation.

Informationssäkerhetskulturen stärks genom att:

- ledningen är engagerad och stöttande.
- återkommande utbildningar ges.
- det finns tydliga rutiner för incidentrapporteringar och uppföljningar av dessa.

- samverkan mellan verksamheterna.
- det finns en öppenhet kring lärdomar av inträffade händelser.

10. Utbildning

Utbildning i informationssäkerhet är en viktig och central roll i informationssäkerhetsarbetet. Målbilden är att alla medarbetare, chefer och förtroendevalda ska ha tillräcklig kunskap för att hantera information på ett säkert sätt för att bidra till en god informationssäkerhetskultur.

Utbildning syftar till att ge höjd kunskap och medvetenhet om aktuella och digitala hot, fysisk informationssäkerhet, incidentrapportering och gällande lagstiftning.

Laholms kommun tillhandahåller utbildning i informationssäkerhet. Utbildningen är obligatorisk för alla anställda och nyanställda och genomförs årligen för samtliga medarbetare under året.

Kommunstyrelsen ansvarar för att det i Laholms kommun, inklusive de kommunägda bolagen, finns en kommungemensam plan för informations- och utbildningsinsatser i informationssäkerhet.

11. Informationsklassning

För att kunna skydda information på rätt sätt behöver vi veta vilken typ av information som hanteras och hur viktig den är. Det görs via informationsklassning som är en metod för att bedöma hur känslig informationen är, hur beroende verksamheten är av den, och vilka konsekvenser det skulle få om den blev fel, otillgänglig eller kom i orätta händer.

Informationsklassning hjälper Laholms kommun att:

- avgöra vilka skyddsåtgärder som krävs.
- skydda sin information på lagom nivå.
- styra behörigheter och åtkomst.
- planera backup, lagring och arkivering.
- följa lagar och regelverk.
- inför upphandling för att få en rimlig kravställning.

Varje förvaltning ska informationsklassa den information som hanteras inom den egna verksamheten. Informationsklassning ska göras i det gemensamma verktyget för att bedöma informationens skyddsvärde.

Informationsklassning ska uppdateras:

- Årligen,
- och vid större förändringar.

12. Riskhantering

Att hantera risker är en viktig del av Laholms kommuns arbete med informationssäkerhet. Riskhantering handlar om att i förväg identifiera vad som kan gå fel, förstå vilka konsekvenser det kan få, och vidta nödvändiga åtgärder för att minska risken att det händer.

Riskhantering ska vara en naturlig del av Laholms kommuns arbete och genomföras:

- när nya system eller tjänster införs.
- vid förändringar i verksamheten eller i olika informationsflöden.
- i samband med informationsklassning.

Riskanalysen ska dokumenteras och innehålla:

- vilka hot och sårbarheter som finns.
- hur sannolikt det är att något inträffar.
- vilka konsekvenser det skulle få.
- vilka åtgärder som behövs för att minska risken.
- identifierade risker som accepteras.

Kommunen ska använda en gemensam metod för riskhantering inom informationssäkerhet. Metoden ska vara samordnad med kommunens arbete med informationsklassning för att säkerställa enhetlighet och effektiv uppföljning.

Riskanalyser ska dokumenteras och förvaras på ett säkert sätt inom kommunens egna system.

13. Upphandling

Vid upphandling av IT-system, digitala tjänster, eller andra tjänster som hanterar information är det viktigt att Laholms kommun ställer krav på informationssäkerhet.

Cybersäkerhetslagen innebär att Laholms kommun måste ha kontroll över sina leverantörer och säkerställa att de uppfyller krav på säkerhet, incidenthantering och efterlevnad av lagstiftning. Denna kontroll sträcker sig under hela avtalets giltighetstid.

Vid upphandling ska Laholms kommun:

- bedöma leverantörens säkerhetsnivå innan avtal tecknas. I dagsläget kan det kommungemensamma informationsklassningsverktyget användas för att få en passande kravställning för det system som ska upphandlas.
- ställa krav på säkerhetsrutiner, incidentrapportering, loggning och åtkomstkontroll.
- följa upp att leverantören lever upp till avtalsbundna säkerhetskrav.
- dokumentera risker och säkerhetsbedömningar kopplade till leverantören.
- samverka med leverantören vid säkerhetsincidenter eller förändring i riskbilden.

Informationssäkerhet och dataskydd (GDPR) vid upphandling.

Vid upphandling kan informationssäkerhets- och dataskyddsaspekter samordnas. Riskbedömning av informationssäkerhet enligt cybersäkerhetslagen och konsekvensbedömning enligt dataskyddsförordningen (GDPR) kan genomföras samordnat och parallellt, med gemensam beskrivning av system, behandling och identifierade hot.

Bedömningarna ska dock hållas åtskilda i syfte och dokumentation, eftersom de utgår från olika regelverk och riskperspektiv. Resultaten ska tillsammans ligga till grund för kravställning i upphandlingen.

Detta innefattar att:

- informationssäkerhetskrav och dataskyddskrav ska beaktas parallellt i upphandlingsprocessen.
- riskbedömningar avseende informationssäkerhet och behandling av personuppgifter kan samordnas, men de ska bedömas och dokumenteras utifrån respektive regelverk.

14. Incidenthantering

Incidenthantering är en viktig del i Laholms kommuns arbete med informationssäkerhet. Syftet är att snabbt kunna upptäcka, hantera och följa upp händelser som kan påverka informationens konfidentialitet, riktighet och tillgänglighet.

En informationssäkerhetsincident kan vara allt från ett misstänkt intrång, en förlorad dator, ett felaktigt e-postutskick eller en störning i ett IT-system. Alla incidenter, oavsett dess omfattning, ska tas på allvar och rapporteras via kommunens utsedda kanaler för incidentrapportering.

Informationssäkerhetsincidenter ska rapporteras omedelbart. Det är bättre att det görs anmälningar om incidenter som senare skulle visa sig inte vara en incident, än att en incident får pågå utan att någon anmäler den. Återkoppling till anmälaren ska alltid ges.

Incidenter ska rapporteras om:

- information har läckt, förlorats eller hamnat i orätta händer.
- obehöriga har fått åtkomst till system eller information.
- system har drabbats av driftstörningar, intrång eller skadlig kod.
- misstanke finns att säkerhetsrutiner inte har följts.
- obehöriga har släppts in i Laholms kommuns lokaler.
- datorer och andra inloggade enheter har lämnats olåsta eller obevakade.

Vissa incidenter kan omfattas av lagstadgad rapporteringsskyldighet. Nedanstående tabell anger tidsramar:

Typ av incident	Enligt lag	Tidsfrist	Rapportering externt
Personuppgiftsincident	Dataskyddsförordningen (GDPR)	Utan onödigt dröjsmål, senast 72 timmar.	Utsedd tillsynsmyndighet

Betydande incident	Cybersäkerhetslagen (CSL)	Upplysning om incident, senast 24 timmar.	Utsedd tillsynsmyndighet
--------------------	---------------------------	---	--------------------------

Alla incidenter ska dokumenteras och följas upp för att identifiera orsaker, sårbarheter och att vidta lämpliga åtgärder och därmed förebygga att liknande händelser sker igen.

Incidenter som påverkar verksamhetens förmåga att upprätthålla kontinuitet ska även hanteras enligt kommunens kontinuitetsplanering.

Roller	Ansvar
Kommunstyrelsen	Ansvarar för att det finns en gemensam modell för alla typer av incidentrapporteringar, inklusive informationssäkerhetsincidenter.
Nämnderna	Har det yttersta ansvaret att informationssäkerhetsincidenter inom den egna verksamheten hanteras korrekt, åtgärdas och följs upp.
Informationssäkerhetssamordnaren	Ansvarar för att samordna incidenthanteringen, ge stöd vid analys och vid betydande incident rapportera vidare till berörd myndighet.
Alla medarbetare	Har ett ansvar att omedelbart rapportera misstänkta eller bekräftade incidenter.

För detaljerad hantering se "Handbok för hantering av personuppgifts- och informationssäkerhetsincidenter", DNR KS 2023:000375.

15. Fysiskt skydd

I informationssäkerhetsarbetet krävs det att det finns fysiskt skydd för att säkra upp utrustning, lokaler och andra tillgångar från obehörig åtkomst, skada, förlust eller störningar.

Fysiskt skydd omfattar:

- tillträdeskontroll till lokaler där känslig information eller IT-utrustning förvaras.
- låsning och förvaring av datorer, dokument och annan utrustning.
- skydd mot brand, vatten, stöld och sabotage.
- begränsad åtkomst till serverrum, arkiv och andra skyddsvärda utrymmen.
- rutiner för besökare, inklusive registrering och ledsagning vid behov.

Exempel på åtgärder:

- datorer och mobila enheter ska alltid låsas när de lämnas obevakade.
- pappersdokumentation med känsligt innehåll ska förvaras i låsta skåp.
- obehöriga personer får inte vistas i Laholms kommuns lokaler utan godkänd ledsagning.

Fysiskt skydd ska anpassas efter informationsklassning och riskbedömningar.

16. Uppföljning och förbättring

Uppföljning är en viktig del i det systematiska informationssäkerhetsarbetet. Syftet är att säkerställa att beslutade säkerhetsåtgärder fungerar som avsett, att identifiera brister och att kontinuerligt förbättra skyddet av Laholms kommuns informationstillgångar.

Resultatet av uppföljningen ska dokumenteras och ligga till grund för förbättringsåtgärder inom ledningssystemet för informationssäkerhet (LIS). Identifierade brister och risker ska hanteras inom ramen för Laholms kommuns reglemente för intern kontroll.

Varje nämnd och bolagsstyrelse ska följa upp att riktlinjen för informationssäkerhet efterlevs årligen och ha löpande kontroll av risker, incidenter och säkerhetsåtgärder.

Uppföljningen ska omfatta:

- Att informationsklassning genomförs.
- Att riskhantering genomförs vid förändringar, införande av nya system och i samband med informationsklassning.
- Att säkerhetsåtgärder som beslutats i riskanalyser är genomförda eller planerade.
- Att informationssäkerhetsincidenter har hanterats.
- Att leverantörer följs upp enligt avtalade säkerhetskrav.
- Att medarbetare och chefer genomför obligatorisk utbildning i informationssäkerhet.

Uppföljningen ska genomföras enligt kommungemensam rutin och stödmaterial som tillhandahålls av kommunstyrelsens förvaltning.

Kommunstyrelsen följer upp informationssäkerhetsarbetet i samband med årsredovisningen.

Kommunstyrelsen ska minst en gång per mandatperiod pröva om styrdokumentet är aktuellt. Om styrdokumentet inte är aktuellt ska det upphävas, revideras eller sammanföras med annat styrdokument vid behov.