Riktlinje

För informationssäkerhet, IT-säkerhet och dataskydd

Herrljunga kommun

Dokumentinformation

Diarienummer:	KS-2024-00284
Fastställd:	Kommunstyrelsen 2025-08-21 § 138
Senast reviderad:	Kommunstyrelsen 2025-08-21 § 138
Giltig till:	Tills vidare
Dokumentansvarig:	Informations- och säkerhetssamordnare

Innehållsförteckning

1. Inledning 4
2. Syfte 4
3. Mål 4
4. Omfattning 5
5. Informationstillgångar 5
5.1 Informationssäkerhet 5
5.2 IT-säkerhet 6
5.3 Dataskydd 6
5.4 LISD 6
5.5 Informationsklassning 6
6. Lagkrav och bestämmelser 7
7. Ansvar och roller 7

1. Inledning

I dagens digitala samhälle är det avgörande att skydda våra informationstillgångar mot olika hot och risker. Information är en värdefull resurs som behöver skyddas så att rätt information är tillgänglig för rätt person vid rätt tillfälle. Informationssäkerhet och dataskydd är avgörande för att Herrljunga kommun ska kunna genomföra sina uppdrag utan störningar, samt skapa motståndskraft och förmåga till återhämtning vid eventuella störningar.

Ett systematiskt informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering, vilket skapar förtroende både inom och utanför organisationen. Information kan kommuniceras, lagras, förädlas, förmedlas, sprida kunskap och styra processer – information behövs för det mesta som en kommun gör. En del information är värdefull, både för organisationer och för den enskilda människan. Om informationen förloras eller är felaktig kan det få allvarliga konsekvenser.

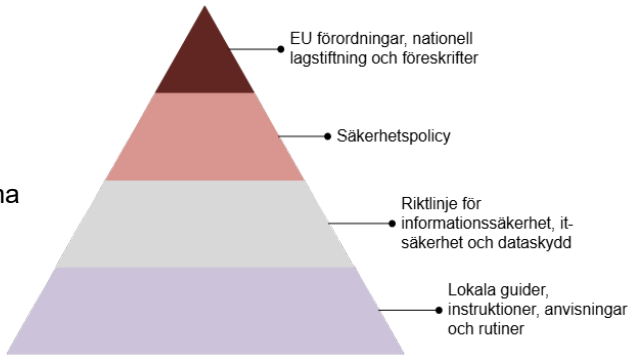
Informationen ska skyddas genom att tillämpa principerna:

- **Konfidentialitet** – att endast behöriga personer får ta del av informationen och att den skyddas från obehörig insyn.
- **Riktighet** – att vi kan lita på att informationen är korrekt och inte manipulerad eller förstörd.
- **Tillgänglighet** – att informationen alltid finns tillgänglig när vi behöver den.

Skyddet ska anpassas efter skyddsbehovet för att vara effektivt, lätt att använda och kostnadseffektivt. Konsekvenserna av bristande skydd är för allvarliga för att ignoreras. Brister i informationshanteringen leder bland annat till minskat förtroende för våra tjänster och för oss som kommun.

2. Syfte

Riktlinjen konkretiserar den övergripande Säkerhetspolicyn. Riktlinjen beskriver gemensamma förutsättningar för ett systematiskt, riskbaserat och integrerat arbete med informationssäkerhet och dataskydd baserat på Säkerhetspolicyn.



3. Mål

Herrljunga kommuns informationssäkerhetsmål är att:

- Kommunens information alltid är identifierad, kartlagd och klassificerad samt har ett ändamålsenligt skydd.
- Informationssäkerhetsrisker som identifieras i organisationen ska hanteras effektivt.
- Organisationen har en god informationssäkerhetskultur där medarbetare och chefer har tillräcklig kompetens, tar ansvar, följer styrdokument och rapporterar brister.
- Kommunen har förmåga att bedriva sin verksamhet även vid incidenter eller störningar.
- Organisationen utvärderar effekten av sitt ledningssystem genom mätning, uppföljning samt interna revisioner.

För att nå dessa mål ska respektive förvaltning:

- Tillsätta resurser inom den egna organisationen för att säkerställa ett effektivt och systematiskt arbete med informationssäkerhet och dataskydd, med fokus på ständig förbättring.
- Identifiera och dokumentera tillämpliga krav på informationssäkerhet och dataskydd, samt säkerställa att organisationen efterlever dessa.
- Kartlägga hur verksamhetens information hanteras och lagras, med utgångspunkt i verksamhetens processer.
- Skydda verksamhetens information på lämplig nivå utifrån klassificering, riskanalys och riskacceptans.
- Utse informationsägare och ansvar för informationstillgångar inom organisationen.
- Kartlägga verksamhetens personuppgiftsbehandlingar och säkerställa ett gott dataskydd, så att personuppgifter hanteras på ett sätt där individens rättigheter tillvaratas lagenligt och korrekt.
- Bedriva kontinuitetsarbete så att verksamheten kan fortgå även vid en allvarlig incident eller störning.
- Kontinuerligt utbilda medarbetare inom informationssäkerhet och dataskydd.
- Omsätta de strategiska informationssäkerhetsmålen i konkreta och mätbara kortsiktiga mål.

4. Omfattning

Riktlinjen gäller för alla förvaltningar inom Herrljunga kommun. Den omfattar medarbetare, extern personal, förtroendevalda och andra som ges tillgång till kommunens informationstillgångar. Riktlinjen gäller även kommunens avtalsparter där det i avtalet anges att kommunens regelverk ska följas.

5. Informationstillgångar

Informationstillgångar omfattar all information och de resurser som krävs för att hantera denna information, såsom IT-system, IT-infrastruktur, pärmar och papper. Oavsett om informationen hanteras manuellt eller automatiserat, och oavsett dess form eller miljö, måste informationstillgångarna skyddas på ett ändamålsenligt sätt**.** Informationssäkerhet och dataskydd är integrerade perspektiv i våra arbetssätt och dagliga rutiner.

Invånarna förväntar sig att kunna sköta sina ärenden snabbt, enkelt och säkert via digitala kontaktvägar. Korrekt hantering av information är avgörande för att upprätthålla tillit och förtroende mellan kommunen och dess invånare, företag och organisationer. Det är också viktigt att information är tillgänglig när den behövs, samt att känslig information skyddas, för att vi ska kunna fullgöra vårt samhällsuppdrag. Därför är informationssäkerhet en central aspekt för alla kommunens verksamheter. Arbetet med informationssäkerhet och dataskydd ska vara en del av kommunens lednings- och kvalitetsarbete, och det omfattar alla informationstillgångar och personuppgifter.

5.1 Informationssäkerhet

Informationssäkerhetsarbetet innebär att införa och förvalta administrativa regelverk, såsom policydokument och riktlinjer, samt att hantera IT-säkerhet, dataskydd och fysisk säkerhet, exempelvis skal- och brandskydd.

Informationssäkerhet är teknikneutral och omfattar skydd av muntlig, pappersburen och digital information. Kommunens arbete utgår från etablerade standarder, såsom SS-ISO/IEC 27000-serien,

dataskyddsförordningen (GDPR) och andra relevanta lagar. Detta är i linje med Myndigheten för samhällsskydd och beredskaps (MSB) rekommendationer för offentlig förvaltning.

5.2 IT-säkerhet

IT-säkerhet består av tre huvudsakliga delar:

- System – tekniska lösningar som brandväggar, klientskydd och andra digitala skydd.
- Rutiner – regelverk och arbetsmetoder som möjliggör ett säkert arbetssätt.
- Organisation – tydlig fördelning av ansvar, roller och uppgifter, från politisk nivå till varje enskild medarbetare.

IT-säkerhet, eller informationstekniksäkerhet, handlar om att skydda information och IT-system mot obehörig åtkomst, manipulation, förstörelse eller stöld. Det omfattar ett antal tekniska och organisatoriska åtgärder för att skydda organisationens värdefulla tillgångar, såsom information, hårdvara (maskinvara) och mjukvara (programvara).

5.3 Dataskydd

Dataskydd handlar om att värna individers grundläggande rättigheter och friheter, särskilt rätten till skydd av personuppgifter. Dataskyddsförordningen (GDPR) gäller i hela EU och syftar till att skapa en enhetlig och hög skyddsnivå för personuppgifter, vilket möjliggör ett fritt flöde av uppgifter inom Europa. Den nationella regleringen, lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, som även kallas för dataskyddslagen, tillsammans med flera andra lagar styr hur kommunens verksamheter får hantera personuppgifter.

5.4 LISD

För att arbeta strukturerat med informationssäkerhet och dataskydd finns ett ledningssystem för informationssäkerhet och dataskydd (LISD). Systemet baseras på standardserien SS-ISO/IEC 27000. Kommunens arbete med implementering och tillämpning utgår från stödmaterial som tagits fram av Myndigheten för samhällsskydd och beredskap (MSB) i samverkan med andra myndigheter.

5.5 Informationsklassning

Utgångspunkten är att kommunens allmänna handlingar ska vara förtecknade i kommunens informationshanteringsplaner (IHP). Dessa planer utgör därför en god grund för vilken information som behöver värderas och klassificeras för att säkerställa en korrekt skyddsnivå.

Med informationstillgångar avses all information samt de resurser som krävs för att hantera den. Det inkluderar allt från IT-system och databaser till manuella register och fysiska dokument. Oavsett form eller lagringsmiljö ska informationen skyddas på ett ändamålsenligt sätt.

Grunden för vårt arbete med att skydda informationstillgångar är kommunens klassningsmodell, som utgår från Sveriges Kommuner och Regioners (SKR) KLASSA. Vi använder deras bedömningsmatris, med anpassade definitioner av konsekvens- och skyddsnivåer, för att systematiskt identifiera och värdera informationens skyddsbehov. De nationella definitionerna har justerats för att spegla kommunens specifika förutsättningar. Varje informationstillgång klassificeras utifrån tre skyddsaspekter: konfidentialitet, riktighet och tillgänglighet.

Genom att klassa informationstillgångar utifrån dessa aspekter identifieras vilka konsekvenser bristande skydd kan medföra, och kraven på informationssäkerhet och dataskydd kan säkerställas.

Syftet med klassningen är att ge ett tillräckligt skydd för kritiska informationstillgångar samtidigt som överskydd och onödiga kostnader undviks. Klassningsmodellen skapar en gemensam ram för enhetlig klassning inom hela organisationen, vilket säkerställer att likvärdiga informationstillgångar får samma skyddsnivå.

6. Lagkrav och bestämmelser

Några av de mest framträdande kraven som normerar arbetet med informationssäkerhet återfinns i följande standarder och författningar:

- **Dataskyddsförordningen (GDPR)**: Ställer krav på systematiskt informationssäkerhetsarbete för att skydda enskildas grundläggande fri- och rättigheter.
- **Dataskyddslagen (2018**:**218)**: Ställer kompletterande bestämmelser till dataskyddsförordningen.
- **NIS-direktivet (EU) 2016/1148**: Syftar till att upprätthålla kontinuiteten i samhällsviktiga tjänster och begränsa hoten mot nätverks- och informationssystem.
- **Tryckfrihetsförordningen (1949:105) och Offentlighets- och sekretesslagen (2009:400) (OSL)**: Kräver systematiskt informationssäkerhetsarbete för att trygga offentlighetsprincipen och förhindra röjandet av sekretessbelagda uppgifter.
- **Säkerhetsskyddslagen (2018:585)**: Ger särskilt skydd för information som är sekretessbelagd med hänsyn till Sveriges säkerhet.
- **Arkivlagen (1990:782)**: Säkrar riktigheten och tillgängligheten hos allmänna handlingar över tid.
- **HSL-FS 2016:40**: Socialstyrelsens föreskrifter om journalföring och behandling av personuppgifter inom hälso- och sjukvården.
- **MSBFS 2020:6**: Föreskrifter om informationssäkerhet för statliga myndigheter, som även kan vara en utgångspunkt för Herrljunga kommuns arbete.
- **MSBFS 2020:7**: Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter, tillsammans med ISO/IEC 27000-standard.
- **ISO/IEC 27000**: Standarder som beskriver ett systematiskt och riskbaserat arbete med informationssäkerhet med stöd av ett ledningssystem.

7. Ansvar och roller

Ansvarsfördelningen för kommunfullmäktige, kommunstyrelsen, nämnder med förvaltningar, kommunala bolag, kommundirektör, verksamhetschefer och medarbetare fastställs i Säkerhetspolicyn. För att upprätta ett effektivt arbete med informationssäkerhet, IT-säkerhet och dataskydd krävs ytterligare tydliggörande av roller, ansvar och befogenheter inom kommunen enligt nedan.

Informationsägaren ansvarar utifrån sitt ordinarie verksamhetsansvar för att informationen hanteras, skyddas och används korrekt enligt verksamhetens behov samt för att säkerhetsåtgärder implementeras och efterlevs utifrån kraven på skydd av informationstillgångar.

Personuppgiftsansvariga (PUA) är kommunens nämnder som ansvarar för respektive verksamhetsområde. Det innebär att nämnderna självständigt bär det yttersta ansvaret för att varje personuppgiftsbehandling sker i enlighet med dataskyddsförordningens regler och principer.

Medarbetare ansvarar för att följa kommunens styrdokument – inklusive policyer, riktlinjer och guider – inom informationssäkerhet, IT-säkerhet och dataskydd. De har även ett ansvar att uppmärksamma och rapportera brister eller incidenter som rör informationssäkerhet och dataskydd till närmaste chef.

Dataskyddsombud (DSO) utses av kommunstyrelsen. Dataskyddsombudet bevakar att personuppgiftsansvariga följer dataskyddsförordningen och annan relevant lagstiftning. Detta sker genom rådgivning, utbildning, vägledning samt olika former av granskningar.

Informationssäkerhetssamordnaren (CISO) ansvarar för att utveckla, leda, samordna och granska informationssäkerhetsarbetet i kommunen. Detta inkluderar arbete med ledningssystemet för informationssäkerhet och dataskydd (LISD) samt regelbunden rapportering till kommunstyrelsen och kommundirektören.

Dataskyddskontakt (DSK) är en funktion som agerar kontaktperson gentemot dataskyddsombudet och arbetar både strategiskt och operativt med dataskydd i kommunen (tidigare benämnd Central registeransvarig). I Herrljunga kommun innehas rollen av informationssäkerhetssamordnaren.

Styrgruppen för informationssäkerhet samordnar och följer upp arbetet med informationssäkerhet och dataskydd. Informationssäkerhetssamordnaren och IT-säkerhetsansvarig är sammankallande och leder arbetet. I styrgruppen ingår IT-chef, kanslichef och säkerhetschef. Beroende på aktuella frågor kan även andra personer kallas till styrgruppsmöten. Styrgruppen sammanträder fyra gånger per år.

Informationssäkerhetshandläggare ska utses inom varje förvaltning (tidigare kallad registeransvarig) och ansvarar för informationssäkerhet och dataskydd inom den egna verksamheten. Funktionen ska arbeta aktivt med dessa frågor och ingår i kommunens informationssäkerhetsnätverk.

Nätverket för informationssäkerhet består av kommunens informationssäkerhetssamordnare, IT-säkerhetsansvarig och informationssäkerhetshandläggare. Nätverket sammankallas av informationssäkerhetssamordnaren och träffas en gång per månad för gemensamt arbete, erfarenhetsutbyte och kompetenshöjande insatser.

IT-chefen ansvarar för kommunens interna tekniska IT-miljö och ska säkerställa att den är både tillförlitlig och säker. Det innebär att IT-miljön uppfyller krav på informationssäkerhet och dataskydd – både internt och gentemot leverantörer. IT-chefen har ett övergripande ansvar för att skydda all information som hanteras inom IT-verksamheten.

IT-säkerhetsansvarig ansvarar för säkerheten i den interna IT-miljön, inklusive arbetssätt, tjänster, processer, system, infrastruktur och verktyg. Funktionen ska säkerställa att säkerhetsnivån är tillräcklig och att den uppfyller verksamhetens krav, lagstiftning samt säkerhetspolicyn och tillhörande styrdokument. IT-säkerhetsansvarig och informationssäkerhetssamordnare ska samverka nära. IT-säkerhetsansvarig arbetar även med att öka säkerhetsmedvetenheten inom IT-området, samordnar och stöttar informationsägare i valet av relevanta säkerhetsåtgärder samt deltar i informationsklassning och kravställning vid upphandlingar.