Region Halland

Informationsklassificering

Hitta i dokumentet

Syfte
Bakgrund
När informationsklassificering ska genomföras
Praktiskt genomförande
Säkerhetsåtgärder
Kravmall
Vid behandling av personuppgifter
Konsekvensnivåer
Referenser och bilagor
Uppdaterat från föregående version

Syfte

Rutinen förklarar hur vi arbetar med informationsklassificering i Region Halland och när den ska genomföras. Informationsklassificering tydliggör informationens värde och därmed skyddsbehov.

Bakgrund

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för informationstillgångar. Alla informationstillgångar, det vill säga information och de resurser som hanterar information ska värderas utifrån verksamhetens behov samt externa krav i form av lagstiftning, avtal och överenskommelser.

Informationsklassificering är en grundläggande aktivitet inom det systematiska informationssäkerhetsarbetet och innebär att all information som hanteras inom Region Halland ska värderas utifrån konfidentialitet, riktighet och tillgänglighet. Klassningen styr vilket skydd information behöver, hur information ska lagras och överföras, samt vilka som ska vara behöriga att ta del av och hantera informationen.

Klassificeringsmodellen baseras på de tre vedertagna informationssäkerhetsaspekterna:

- **Konfidentialitet** - Att information inte tillgängliggörs eller avslöjas för obehöriga.
- **Riktighet** - Att information är korrekt, aktuell och fullständig.
- **Tillgänglighet** - Att information kan nås när den behövs av behöriga användare.

Aspekten ”spårbarhet” klassas inte utan hanteras som en säkerhetsåtgärd för att tillgodose krav på konfidentialitet och riktighet.

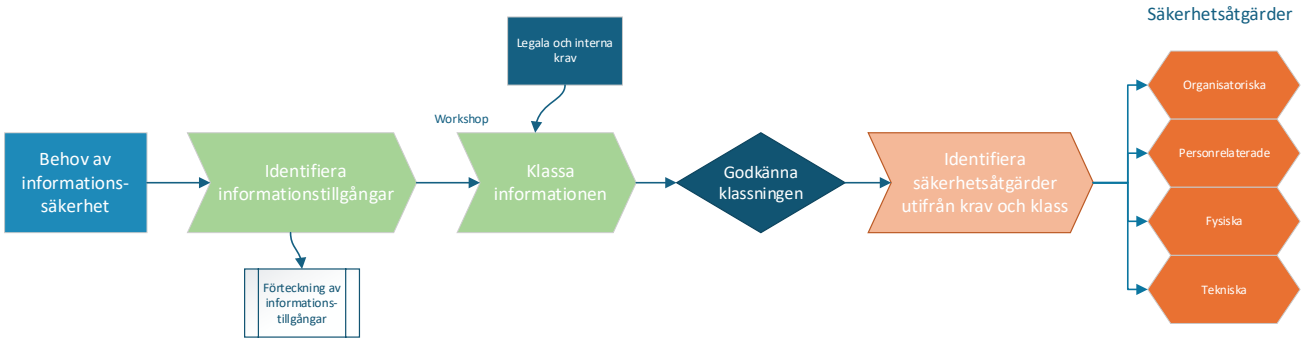
När informationsklassificering ska genomföras

All information som hanteras inom Region Halland ska informationsklassificeras. Det ska också genomföras när system- eller informationsmängder uppstår, förändras eller då lagkrav tillkommer eller ändras. Inom regionen är det verksamheten som ansvarar för att identifiera vilken information som finns och fastställa dess betydelse för verksamheten. Det är system-

och/eller informationsägaren som ansvarar för att det genomförs en informationsklassificering.

Praktiskt genomförande

Region Halland använder systemstödet KLASSA för att praktiskt genomföra informationsklassificering. Den genomförs lämpligast i workshop-format där exempelvis systemägare, verksamhetschef och utvecklare deltar. Beroende på system eller informationsmängd kan även andra roller bli aktuella att bjuda in. Stöd kan tas av utsedd kontaktperson för informationssäkerhet i förvaltningen eller specialist på Informationssäkerhetsavdelningen, Regionkontoret. Metodstöd finns framtaget att använda inför och under en klassnings-workshop.



Säkerhetsåtgärder

Informationsklassificering är en nödvändig utgångspunkt för riskhanteringsarbetet. Genom att klassificera informationen baserat på dess skyddsvärde och hotnivå kan därefter lämpliga säkerhetsåtgärder väljas samt krav fastställas för hur informationen ska hanteras.

Säkerhetsåtgärderna kan vara:

- Organisatoriska
- Personrelaterade
- Fysiska
- Tekniska

Konkreta användningsområden där en informationsklassificering ska ligga till grund för val av säkerhetsåtgärder är till exempel:

- Kravställning inför upphandling av system
- Utveckling av ett informationssystem eller tjänst
- Fastställande av hanteringsregler för information, till exempel krav på kryptering, märkning av information, kommunikation via mobiltelefon etcetera.

Informationsägaren eller dess representant samverkar med lämplig funktion inom IT- och Digitalisering kring vilka åtgärder som är ändamålsenliga och proportionerliga.

Kravmall

För att fastställa skyddsbehovet för informationstillgångarna är det nödvändigt att identifiera de krav som ställs på varje enskild informationsmängd. Denna process innefattar två huvudtyper av krav: rättsliga krav och interna krav.

- **Rättsliga krav:** Dessa omfattar lagar, förordningar och föreskrifter som reglerar hanteringen av information. Genom att följa dessa krav säkerställs att informationen behandlas lagligt och att skyddsnivån är adekvat.
- **Interna krav**: Organisationen eller verksamheten kan ha specifika krav för sin verksamhet. Dessa interna krav kan vara unika för varje verksamhet och bör beaktas vid informationsklassificering.

Vid behandling av personuppgifter

Om informationen innehåller personuppgifter ska ytterligare analyser genomföras för att bedöma om det finns behov av att göra ett PUB-avtal och/eller konsekvensbedömning (DPIA) avseende personlig integritet. Syftet med konsekvensbedömning är att förebygga risker innan de uppkommer samt säkerställa att integriteten för de registrerade värnas.

Konsekvensnivåer

De konsekvensnivåer som används i KLASSA följer den modell för klassificering av information som utarbetats av Myndigheten för civilt försvar och Svenska Institutet för Standarder (SIS).

0. **Ingen eller försumbar skada**
   Inga konsekvenser och i regel publik information, tex intranätet.

1. **Måttlig skada**
   Kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för Regionen eller tredje part.

2. **Betydande skada**
   Kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för Regionen eller tredje part.

3. **Allvarlig skada**
   Kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarlig skada för Regionen eller tredje part.

4. **Av betydelse för Sveriges säkerhet**
   I samband med informationsklassificering där konsekvensnivån är hög kan indikation uppstå om enskilda informationstillgångar även kan ha en påverkan på Sveriges säkerhet (nivå 4). Det kan handla om att viss information och/eller aggregerad

information har ett skyddsvärde som faller under Säkerhetsskyddslagen eller att tillgänglighet och/eller riktighet har en så stor betydelse att hela eller del av tjänst har betydelse för Sveriges säkerhet. Vid sådan indikation ska den som är ansvarig för informationsklassificeringen kontakta Signalskydds- eller Säkerhetsskyddschef.

Referenser och bilagor

- KLASSA SKR
- Riktlinje för informationssäkerhet

Uppdaterat från föregående version

Ny rutin.