Gäller för: Västra Götalandsregionen
Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör
Giltig från: 2024-08-05
Giltig till: 2028-07-24

Informationsklassning

Regional rutin 2024 – 2028

Ledningssystem för informationssäkerhet och dataskydd

Rubrik: Informationsklassning - Regional rutin 2024 - 2028
Dokument-ID: RS10162-1596316381-102
Version: 4.0

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

Sammanfattning

Mål: Verksamheten ska identifiera vilken information och andra relaterade informationstillgångar som finns och fastställa dess betydelse för verksamheten.

Informationsklassning är en grundläggande aktivitet i det systematiska informationssäkerhetsarbetet. Informationsklassning innebär att informationen värderas utifrån vilka konsekvenser ett otillräckligt skydd av informationens konfidentialitet, riktighet och tillgänglighet skulle kunna få. Klassningens resultat visa r på vilket skyddsbehov informationstillgångarna har för verksamheten och därmed vilka krav som ställs på informationens konfidentialitet, riktighet och tillgänglighet. Resultatet av klassningen är ett underlag för att kunna gå vidare med att välja lämpliga säkerhetsåtgärder.

Regional rutin informationsklassning är styrande för alla förvaltningar och bolag i Västra Götalandsregionen och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD). Rutinen fastställer den modell för klassning som ska användas av verksamheten. För det praktiska genomförandet finns ytterligare stödmaterial som vägledning, mall och presentationsmaterial.

Alla informationstillgångar ska ha en utpekad informationsägare under hela tillgångens livstid. Grundprincipen är att informationsägarskapet följer det ordinarie verksamhetsansvaret. Detta gäller från ledning till enskilda medarbetare.

1. Ansvar och roller

1.1 Informationsägare

Informationsägaren ansvarar för att genomföra informationsklassning och riskbedömning för den information som hanteras i dennes verksamhet. Informationsägaren godkänner informationsklassningens resultat. Utifrån informationsklassningen ställer informationsägaren krav på skydd av informationstillgångarna eftersom konsekvenserna av bristande säkerhet uppstår i informationsägarens verksamhetsprocess. I ansvaret ingår även att säkerställa implementation och efterlevnad av säkerhetsåtgärder utifrån krav på skydd för informationstillgångarna.

De interna relationerna mellan informationsägare och ägare av IS/IT-tjänst ska, när det gäller informationssäkerhet, utgå från informationsägarens ansvar för informationen.

1.2 Regional processägare

Vid regiongemensamma processer kan regional processägare företräda informationsägare. Regional processägare ansvarar då för att respektive informationsägares intresse tas tillvara.

1.3 Ägare av IS/IT-tjänst

Respektive IS/IT-tjänst ska ha en ägare. Denne ansvarar för tekniska säkerhetsåtgärder i IS/IT-tjänsten, vilket innebär att införa, förvalta och följa upp utifrån den regionala processägarens alternativt informationsägarens krav på skydd för informationstillgångarna. Det är av största vikt att ägaren har god kännedom om vilken information som behandlas i IS/IT-tjänsten och hur dessa är klassade.

1.4 Projektägare

Informationssäkerhet ska vara en del av projekt. Projektägare ska inledningsvis i ett projekt säkerställa att informationsklassning har genomförts eller se till att det sker, för att kunna fastställa de krav på informationssäkerhet som verksamhetens information kräver.

Projektägare ska i ett tidigt skede identifiera vem som är informationsägare. Då projekt avslutas och övergår i ordinarie linjeverksamhet är det informationsägare som övertar ansvaret för informationssäkerhetsarbetet och därmed informationsklassning.

2. När ska informationsklassning göras

Alla informationstillgångar i verksamheten ska identifieras och klassas. Information har en livscykel, från det att den skapas till att den gallras. Värdet av informationen kan variera under hela livscykeln men informationssäkerheten är viktig i alla stadier av cykeln.

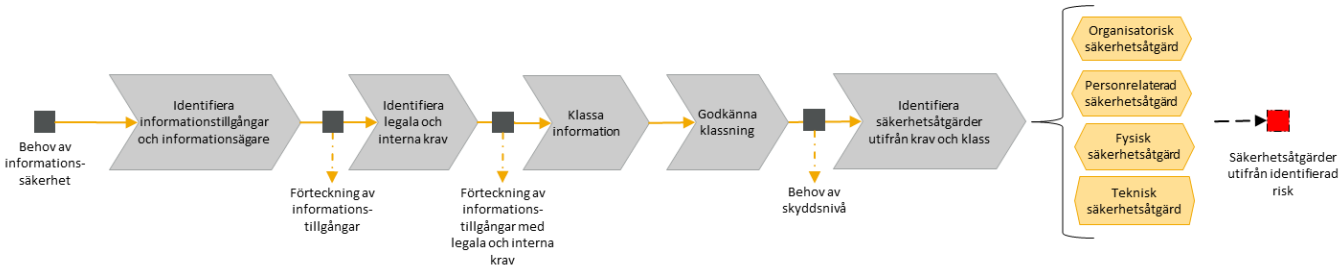
Exempel på situationer när en informationsklassning ska genomföras och ligga till grund för val av lämpliga säkerhetsåtgärder:

- vid organisationsförändringar och förändringar av verksamhetsprocesser som påverkar informationshanteringen.
- när antalet användare av informationstillgången förändras påtagligt.
- vid förändrade interna eller externa säkerhetskrav som påverkar informationsbehandlingen.
- vid ny eller förändrad lagstiftning.
- vid upphandling av IS/IT- tjänst eller vid ny funktionalitet eller utökat användningsområde, eller om IS/IT- tjänsten ska behandla annan information än den ursprungliga klassningen tog hänsyn till.
- vid användning av molntjänster eller outsourcing.
- vid tekniska förändringar i infrastruktur eller programvaror, som kan påverka informationsbehandlingen.

Den regionala processägaren eller informationsägaren ska årligen granska att informationsklassningen fortfarande är gällande. Informationsklassning behöver vara en naturlig del av verksamheten eftersom resultatet av informationsklassning kan påverka budget och/eller verksamhetsplanering.

3. Genomförande

Att klassa information är en regiongemensam process, vilket skapar en gemensam förståelse för informationens skyddsvärde och för tillämpningen av säkerhetsåtgärder.



Figur 1 Regiongemensam process för informationsklassning.

3.1 Identifiera informationstillgångar

Informationstillgångar är den information som är av värde för verksamheten och som ska skyddas med hjälp av informationssäkerhet, inklusive de informationsbehandlingsresurser som behandlar informationen.

Informationsbehandlingsresurs är också en informationstillgång, digital eller fysisk, för behandling av information (till exempel IS/IT-tjänst, infrastruktur, säkerhetsskåp eller medarbetare).

Identifiera vilka informationstillgångar som ska ingå i klassningen. För att göra informationsklassning krävs förståelse för i vilka sammanhang informationen uppstår, hanteras, lagras och bearbetas. Utgå från verksamhetens process, till exempel genom att använda en processbeskrivning, myndighetens klassificeringsstruktur och/eller informationshanteringsplan.

Det är av vikt att tydligt definiera om det finns en avgränsning över vad som ingår i klassningen.

3.2 Identifiera informationsägare

Alla informationstillgångar ska ha en utpekad informationsägare under hela tillgångens livstid. Identifiera vem som är ägare av informationstillgångarna och som senare ansvarar för att godkänna klassningens resultat.

Grundprincipen är att informationsägarskapet följer det ordinarie verksamhetsansvaret. Detta gäller från ledning till enskilda medarbetare. Informationsägarskapet sammanfaller med ansvaret i verksamheten, till

exempel ansvarar en verksamhetschef för information inom verksamheten.

När informationstillgångarna ingår i regiongemensamma verksamhetsprocesser, IS/IT- tjänster, projekt och/eller upphandlingar företräds flera myndigheters informationsägare av en regional processägare. Den regionala processägarens företrädarskap har sin utgångspunkt i de koncernövergripande grupper utifrån beslutet att arbeta processorienterat, gemensamt och sammanhållet.

3.3 Identifiera krav

För att kunna fastställa skyddsbehovet av informationstillgångarna behöver man veta vilka krav som ställs på respektive informationstillgång. Arbetet med att identifiera krav delas upp på dels rättsliga krav i form av lagar, förordningar och föreskrifter, dels på krav som organisationen eller verksamheten ställer för att kunna uppnå sina mål, så kallade interna krav.

3.4 Klassa informationstillgångar

Att klassa informationstillgångarna är att bedöma vilka konsekvenserna blir vid brister i konfidentialitet, riktighet och tillgänglighet.

- Konfidentialitet - egenskap som innebär att informationstillgången inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.
- Riktighet - egenskap som innebär att informationstillgången skyddas mot oönskad förändring.
- Tillgänglighet - egenskap som innebär att informationstillgången är åtkomlig och användbar inom förväntad tid och omfattning.

Bedömning av konsekvensen ska göras utifrån kategorierna:

- individ (hälsa, fri- och rättigheter eller integritet)
- kärnverksamhet (verksamhetens huvudsakliga uppdrag)
- egen eller andras samhällsviktiga funktioner
- organisationens förtroende eller ekonomi

Extra skyddsvärda informationstillgångar

Alla informationstillgångar är inte lika viktiga för verksamheten. Med extra skyddsvärda informationstillgångar avses sådana som stödjer de delar av verksamheten som anses samhällsviktiga eller verksamhetskritiska. Det är av vikt att identifiera om det finns

informationstillgångar som är särskilt kritiska och/eller som kan behöva ett särskilt skydd.

Klassningsmodell

Informationsklassning ska genomföras utifrån regionens fastställda informationsklassningsmodell (figur 2). Vid bedömning är det viktigt att ta hänsyn till om informationen i aggregerad eller ackumulerad form kan skapa ett högre skyddsvärde och/eller om information kan upphöra att vara känslig eller kritisk efter en viss tidsperiod, till exempel när information har offentliggjorts. Dessa aspekter bör beaktas eftersom en för låg klassning kan riskera att informationen inte skyddas i den omfattning den har behov av eller att en för hög klassning kan leda till införande av omotiverade säkerhetsåtgärder.

Klass	Konsekvensnivå	Kategori	Konsekvensbeskrivning
0	**Försumbar**	**Individs hälsa, fri- och rättigheter eller integritet**	Ingen eller försumbar skada på den personliga integriteten för enskild individ, vare sig avseende fysisk, ekonomisk eller integritetsrelaterad skada.
		Kärnverksamhet	Inga svårigheter för verksamheten att nå målen.
		Egen eller andra samhällsviktiga funktioner	Ingen påverkan på samhällsviktiga funktioner.
		Organisationens förtroende och/eller ekonomi	Ingen eller försumbar påverkan på VGR:s förtroende eller ekonomi. Lite negativ uppmärksamhet.
1	**Måttlig**	**Individs hälsa, fri- och rättigheter eller integritet**	Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten men som bör kunna övervinnas trots vissa svårigheter.
		Kärnverksamhet	Inga märkbara större svårigheter för verksamheten att nå målen.
		Egen eller andra samhällsviktiga funktioner	Andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär med endast mindre påverkan.
		Organisationens förtroende och/eller ekonomi	Uppleva lindriga besvär men utan påvisbar ekonomisk eller förtroende påverkan. Enstaka missnöjda individer som uttalar sig i sociala medier, eller en notis i lokalmedia.
2	**Betydande**	**Individs hälsa, fri- och rättigheter eller integritet**	Enskilda personer kan uppleva konsekvenser, såsom stora fysiska eller psykiska besvär eller stor ekonomisk påverkan som de bör kunna övervinna även om det måste ske med reella och allvarliga svårigheter (exempelvis obehörig spridning av personuppgifter i stor omfattning).
		Kärnverksamhet	Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).
		Egen eller andra samhällsviktiga funktioner	Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder), samhällsviktiga funktioner i egen eller annan organisation påverkas i liten utsträckning.
		Organisationens förtroende och/eller ekonomi	VGR kan påverkas, risk för stor skada, risk för ekonomisk skada. Minskat förtroende genom nyheter i både riks- och lokalmedia och i organiserade grupperingar i sociala medier.
3	**Allvarlig**	**Individs hälsa, fri- och rättigheter eller integritet**	Enskilda personers liv och fysiska eller psykiska hälsa äventyras på ett sätt som är oåterkalleligt eller som inte kan övervinnas av den enskilda eller får mycket stora ekonomiska konsekvenser, (exempelvis genom att känsliga personuppgifter sprids till en stor krets obehöriga, skyddade personuppgifter tillgängliggörs eller enskilda riskerar att drabbas av personlig konkurs.
		Kärnverksamhet	Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.
		Egen eller andra samhällsviktiga funktioner	Samhällsviktiga funktioner i egen eller annan organisation påverkas.
		Organisationens förtroende och/eller ekonomi	VGR förlorar förtroende, mycket stor ekonomisk skada. Minskat förtroende exempelvis genom ihållande drev i rikstäckande medier eller av organiserade grupperingar i sociala medier.
4	**Av betydelse för Sveriges säkerhet**	Finns indikation att informationstillgångar omfattas av säkerhetsskyddslagen ska dessa analyseras och hanteras enligt särskilda bestämmelser i enlighet riktlinje och rutin för säkerhetsskydd.	

Figur 2 Klassningsmodell Västra Götalandsregionen (Klassa, Sveriges Kommuner och Regioner).

3.5 Fastställa skyddsnivå

När informationstillgångarna är klassade ska informationsägaren fastställa resultatet genom att godkänna den dokumenterade informationsklassningen. Informationsklassningen dokumenteras i regional mall och upprättas och bevaras hos informationsägarens myndighet i enlighet med myndighetens informationshanteringsplan.

Klassningen ger informationsägaren en värdering av informationens skyddsbehov. Skyddsbehovet ska omhändertas av informationsägaren för

att kunna ställa krav på införande av tillräckliga säkerhetsåtgärder för att uppnå en tillräcklig informationssäkerhet.

3.6 Vid behandling av personuppgifter

Om informationen innehåller personuppgifter ska ytterligare analyser genomföras för att bedöma om det finns behov av att genomföra en konsekvensbedömning avseende personlig integritet. Syftet är att ta reda på om behandlingen av personuppgifter leder till hög risk för de registrerades fri- och rättigheter. Vägledning om analyserna och hur dessa går till finns att läsa i ledningssystemet för informationssäkerhet och dataskydd.

3.7 Identifiera säkerhetsåtgärder

Nästa steg är att identifiera lämpliga säkerhetsåtgärder. Säkerhetsåtgärder är åtgärder för att upprätthålla informationssäkerheten, dessa återfinns i:

- Informationsklassning, i stödmaterial *Vägledning säkerhetsåtgärder* återfinns säkerhetsåtgärder som utgör en grundnivå för den klass som informationstillgången har.
- Krav, i *Vägledning legala krav* återfinns säkerhetsåtgärder som för att möta legala krav. Interna krav återfinns i andra rutiner och styrande dokument inom ledningssystemet för informationssäkerhet och dataskydd.
- Riskhantering, säkerhetsåtgärder identifieras vid behandling av risker i riskhanteringsprocessen.

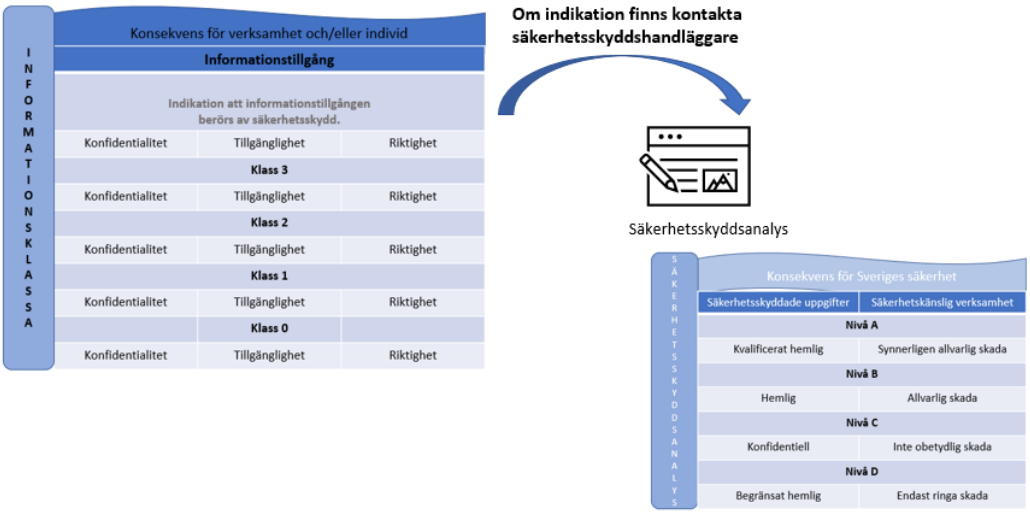
Det är viktigt att informationsägaren inför säkerhetsåtgärder som skyddar informationen tillräckligt, det innebär bland annat att olika säkerhetsåtgärder behöver kombineras.

4. Informationsklassning i förhållande till säkerhetsskyddslagens konsekvensnivåer

Informationsklassning innebär att bedöma konsekvens för konfidentialitet, riktighet och tillgänglighet utifrån ett verksamhets- och individperspektiv. När informationen träffas av säkerhetsskydd bedöms om uppgifter eller verksamhet har en påverkan på Sveriges säkerhet.

I samband med informationsklassning där konsekvensnivån är hög kan indikation uppstå om enskilda informationstillgångar även kan ha en påverkan på Sveriges säkerhet. 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 informationsklassningen kontakta förvaltningens säkerhetsskyddshandläggare för rådgivning.

Vid en bedömning om vad som träffas av säkerhetsskyddslagen görs en värdering av skada utifrån ett antagonistiskt perspektiv och vad som bedöms skyddsvärt utifrån Sveriges säkerhet. För mer information om säkerhetsskydd ta del av riktlinje för säkerhetsskydd.



Figur 3 Informationsklassningsmodellen (till vänster i bild), fastställd i denna rutin, i relation till konsekvensnivåer utifrån Sveriges säkerhet. Matris för konsekvensnivåer för Sveriges säkerhet fastställs i säkerhetsskyddslagen och Säkerhetspolisens föreskrifter.

5. Nästa steg

Det som verksamheten identifierat som skyddsvärda informationstillgångar är ingångsvärdet i arbetet med riskhantering. Riskbedömningen syftar till att ge ett beslutsunderlag om vilka säkerhetsåtgärder som slutligen väljs. Informationsägaren eller dess företrädare ska välja säkerhetsåtgärder som är ändamålsenliga och proportionerliga utifrån det riskbaserade informationssäkerhetsarbetet.

6. Relaterade dokument

- Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet
- Policy - säkerhet och beredskap i Västra Götalandsregionen (dnr RS 2018-00129)
- Informationssäkerhet och dataskydd - Regional riktlinje 2023 – 2027 (dnr RS 2023-02811)
- Informationssäkerhet, cybersäkerhet och integritetsskydd - Kontroller av informationssäkerhet (ISO/IEC 27002:2022)
- Vägledning Säkerhetsåtgärder
- Vägledning legala krav

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-102

Version: 4.0

Giltig från: 2024-08-05

Giltig till: 2028-07-24