Dokumentnamn: Försäkrings AB Göta Lejons rutin för informationsklassning

Beslutad av:	Gäller för:	Diarienummer:	Datum och paragraf för beslutet:
VD	Försäkrings AB Göta Lejon	-	-

Dokumentsort:	Giltighetstid:	Senast reviderad:	Dokumentansvarig:
Rutin	Tills vidare	2025-01-27	Säkerhetschef

Bilagor:
Bilaga 1: Ordlista
Bilaga 2: Utbildningsmaterial informationsklassning

Försäkrings AB Göta Lejons rutin för informationsklassning

Syftet med denna rutin

Denna rutin är ett praktiskt hjälpmedel i arbetet med att genomföra informationsklassningar i enlighet med Göta Lejons anvisning för informationsklassning.

Vem omfattas av rutinen

Denna rutin gäller tills vidare för samtliga medarbetare

Koppling till andra styrande dokument

Styrande dokument gemensamt för staden:

- Göteborgs stads riktlinjer för informationssäkerhet

Styrande dokument Försäkrings AB Göta Lejon:

- Försäkrings AB Göta Lejons anvisning för informationsklassning
- Försäkrings AB Göta Lejons anvisning för säkerhet

Ordlista

Ordlistan är en förklaring av vanligt förekommande begrepp.

Begrepp	Förklaring
Information	Fakta, idéer eller liknande i en form lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
Informationsmängd	En gruppering av information som kan överföras med hjälp av eller lagras på en eller flera informationsbärare.

Informationsbärare	Den hård- eller mjukvara som används när en informationsmängd överförs, behandlas eller lagras. En informationsmängd kan exempelvis inkomma via ett telefonsamtal, då är telefonisystemet informationsbärare. Informationsmängden kan sedan antecknas i ett verksamhetssystem, då är verksamhetssystemet informationsbärare. Informationsbärarna används för att förmedla, bevara och förädla informationsmängden.
Informationstillgång	Information och informationsbärare som är av värde för en organisation. En informationstillgång är summan av informationen och informationsbäraren.
Informationsägare	Den som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten. Informationssägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.
Systemägare	Den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare. Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.
Tillgång	Allt som är av värde för en organisation, exempelvis byggnader, personal, kunskap, applikationer, servrar eller finansiella tillgångar.

Rutin

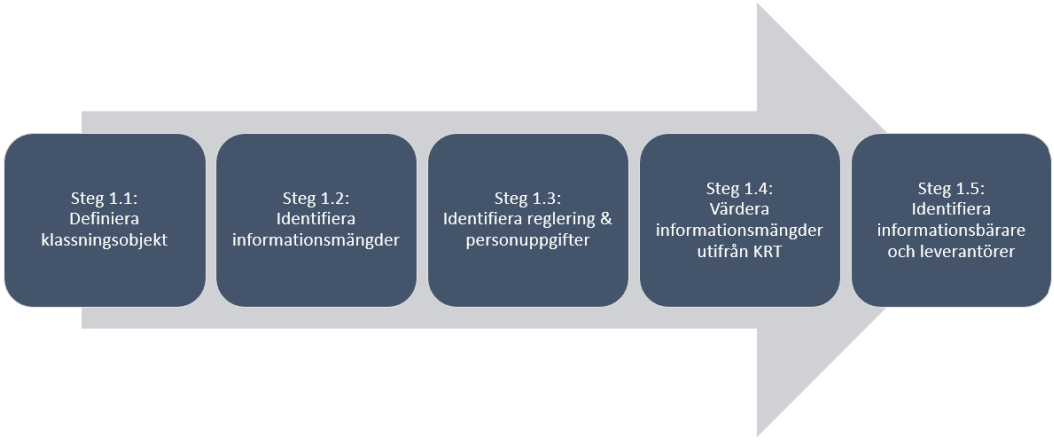
Vad är informationsklassning?

Informationsklassning innebär att man värderar organisationens informationstillgångar utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet.

Syftet är att sätta rätt nivå av säkerhetsåtgärder beroende på informationens värde. Informationsklassning är tillsammans med riskanalyser de viktigaste underlagen för att fatta beslut om tillräckliga säkerhetsåtgärder för att skydda informationen. Hur informationsklassningen förhåller sig till övriga aktiviteter visas i Figur 1.

Figur 1

Figur 2 visar klassningsprocessen (steg 1 i Figur 1) med de steg som behöver genomföras för att kunna avgöra vilka säkerhetsåtgärder som bör finnas på plats utifrån informationens skyddsbehov.



Figur 2

När ska informationsklassning genomföras?

Informationsklassning kan föranledas av:

- Behov av förnyad informationsklassning pga förändringar i process, förändrad användning av informationen i en, eller förändringar i lagar, styrande dokument eller avtal som har påverkan på informationen i processen.
- Skapande eller användande av nya informationsmängder
- Behov av uppdatering av informationsklassning, eftersom detta ska göras minst vart fjärde år.

Vad ska informationsklassas?

Den information som ska klassas är den information som används eller hanteras i de aktiviteter som genomförs i bolagets processer.

Alla processer som klassas ska vara definierade och beskrivna. Om processkarta finns framtagen ska denna användas för att visualisera de steg som genomförs inom processen.

Om klassningen avser ett system är det informationen som används eller hanteras i systemet som ska klassas.

Ansvar

Informationsägaren ansvarar för att klassa informationen. På Göta Lejon är processägare, alltså vd och teamledare, även informationsägare. Processägare är alltså ansvarig för informationsklassning av de processer denna ansvarar för.

För processer som fastställts av annan part, exempelvis av kommunstyrelsen eller kommunfullmäktige, ansvarar den som på Göta Lejon tilldelats ansvar för verkställande av processen även för att klassa informationen.

Informationsägaren kan utse en *informationsklassningsansvarig* som håller i det praktiska arbetet med genomförande av workshop, dokumentation etc. Ansvar och fastställande kan däremot inte överlåtas på informationsklassningsansvarig.

Systemägare ansvarar för att klassa den information som uppkommer och ägs av systemet. Exempel är information så som tekniska specifikationer av systemet, information om säkerhetsfunktioner eller annan information som inte framställs eller hanteras i verksamhetsprocessen. Denna typ av information klassas endast undantagsvis inom Göta Lejons verksamhet.

Informationsägaren ansvarar även för att dokumentera informationsklassningen i Göta Lejons diarie. Alla klassningar dokumenteras under samma ärende. En informationsklassning omfattas sällan av sekretess. Själva beslutet om att informationsklassning ska genomföras behöver inte dokumenteras. Om informationsägaren däremot beslutar att informationsklassning inte ska genomföras ska beslut med motivering dokumenteras i diariet.

Steg 1:1 Definiera klassningsobjekt

Definition av klassningsobjekt är det första steget i klassningen och innebär att allt arbete förbereds inför klassningsworkshopen.

Undersök process

Om det finns en etablerad process eller delprocess enligt Göta Lejons processkartor ska den ligga till grund för informationsklassningsarbetet. Om etablerad process saknas behöver processen först definieras innan eller i samband med workshop. Det behöver som minst finnas en tydlig beskrivning av processen och dess syfte. Det är även bra om det finns en processkarta som tydligt visualiserar de aktiviteter som genomförs, vilket kan tas fram via verktyget 2c8.

Identifiera deltagare

Det är viktigt att rätt kompetens ingår i en klassningsworkshop för att den ska bli effektiv. Processägare/informationsägare kan utse en informationsklassningsansvarig. Utöver dessa roller bör informationsägaren värdera om det även behövs deltagare med domänkunskap inom system, IT, dataskydd, OSL eller andra områden.

Samla in underlag

Inför informationsklassningsworkshopen är det lämpligt att samla in relevanta underlag.

- Informationsklassningsmall som med fördel kan fyllas i med grundläggande information om klassningsobjektet innan workshop.
- Processbeskrivning inkluderat processkarta om sådan är framtagen.
- Lagar eller styrdokument som gäller för processen och som har påverkan på informationshanteringen, exempelvis GDPR eller OSL.
- Avtal eller överenskommelser som reglerar informationshanteringen, exempelvis sekretessavtal eller personuppgiftsbiträdesavtal.
- Eventuella tidigare informationsklassning eller andra genomförda informationsklassningar av liknande art.
- Eventuellt annan information som kan vara av värde för informationsklassningens genomförande, exempelvis bedömningar i dokumenthanteringsplanen eller behandlingsregistret för personuppgifter.

Det underlättar om den som är informationsklassningsansvarig sätter sig in i materialet i förväg. Denne kan då välja bort den information som inte är relevant för just den här informationsklassningen.

Planera workshop informationsklassning

Tänk på att informationsklassning kan vara tidskrävande. Räkna med att det kan ta ca. 6 timmar totalt eller mer beroende på hur komplex processen är. Detta kan sedan delas upp antingen i 2-3 lite längre arbetsmöten eller i flera kortare arbetsmöten, beroende på vad arbetsgruppen föredrar.

Steg 1:2 Identifiera informationsmängder

I detta steg startar workshopen där själva informationsklassningsarbetet genomförs.

Utbilda deltagarna

Starta med en kortare utbildning av deltagarna med hjälp av en presentation, se bilaga 2.

Undersök om processen omfattas av säkerhetsskydd

Säkerhetsskydd innebär att skydda den information och de verksamheter som är av betydelse för *Sveriges säkerhet* mot spionerі, sabotage, terroristbrott och vissa andra hot. Säkerhetsskydd regleras i säkerhetsskyddslagen.

Omfattas den aktuella processen av säkerhetsskydd, avbryts informationsklassningen och bolagets säkerhetsskyddschef kontaktas för fortsatt hantering.

Identifiera informationsmängder

Identifiera de informationsmängder som tillhör varje enskild processaktivitet. I vissa fall hanteras ingen information i processaktiviteten. Gå då vidare till nästa processaktivitet. I andra fall hanteras flera olika informationsmängder i samma processaktivitet. Tänk på att även analog information kan behöva klassas, exempelvis information som finns på papper.

Informationen ska delas upp i informationsmängder, som består av en väl avgränsad mängd information med ett specifikt syfte i processen. Det kan exempelvis vara faktura, konton, beslut, tjänsteutlåtande, rapport etc.

Ibland kan det vara till hjälp att tänka i termer av ingående - behandling - utgående information:

- Vilken information kommer in i aktiviteten?
- Vilken information uppstår eller behandlas i aktiviteten?
- Vilken information går ut ur aktiviteten?

Informationsmängderna ska inte delas upp i mindre beståndsdelar än sin databärare eller handling. Ett papper, en word- eller pdf-fil ska inte delas upp i mindre beståndsdelar.

Notera att det är informationsmängder som ska identifieras, inte eventuella informationsbärare. En informationsmängd kan behandlas av en eller flera informationsbärare men i denna del av informationsklassningsprocessen är det endast informationsmängderna som är av intresse.

Steg 1:3 Identifiera reglering och personuppgifter

Efter att informationsmängderna har identifierats ska varje informationsmängd eller processen som helhet analyseras i syfte att identifiera om informationen omfattas av någon reglering.

Regleringar kan bestå av lagar, förordningar eller föreskrifter men också stadens eller Göta Lejons egna styrdokument. Ibland är det endast enskilda informationsmängder som omfattas av viss reglering och i andra fall kan det vara samtliga informationsmängder i processen.

Några vanligt förekommande regleringar är:

- Tryckfrihetsförordningen (TF)
- Offentlighets- och sekretesslagen (OSL)
- Arkivlagen (ArkivL)
- Dataskyddsförordningen (GDPR)

För den typen av regleringar som endast gäller vissa typer av information så som de som listas i punktlistan ovan ska det tydligt framgå vilka regleringar som är tillämplig för vilken informationsmängd. För lagstiftning som gäller processen i sin helhet räcker det att dokumentera detta på processnivå. För att kunna identifiera och dokumentera detta på rätt sätt är det därför viktigt att någon av deltagarna i workshopen har god kunskap om reglering som gäller för klassningsobjektet.

Identifiera sekretessreglerade uppgifter

För varje informationsmängd som kan förväntas innehålla sekretessreglerade uppgifter ska aktuell paragraf i offentlighets- och sekretesslagen anges. Tillämpliga sekretessregleringar ska fyllas i med formaten ”[kapitel]:[paragraf]”, exempel: 18:8.

Observera att en sekretessprövning alltid måste genomföras i varje enskilt fall.

Några vanligt förekommande sekretessregleringar på Göta Lejon är följande:

Sekretessreglering:
15 § 2 Försvarssekretess
17 § 3b Utredning av rapporter om missförhållanden
18 § 13 Risk- och sårbarhetsanalyser
18 § 8 Säkerhets- eller bevakningsåtgärd
19 § 3 Upphandling
21 § 1 Enskilds hälsa eller sexualliv
31 § 16 Affärsförbindelse med myndighet
38 § 1 Krigsplacering
39 § 3 Adresser, telefonnummer, m.m.
40 § 6 Skaderegleringsverksamhet

Identifiera personuppgifter

Kontrollera om respektive informationsmängd innehåller personuppgifter. En personuppgift är varje form av upplysning som direkt eller indirekt kan kopplas till en fysiskt levande person. Detta innebär att en personuppgift inte bara är något som kan härledas direkt, som ett namn eller personnummer. De omfattar även indirekta personuppgifter som IP-nummer, hälsoinformation eller en unik identifierare i en applikation.

När personuppgifter förekommer ska följande anges, fullständig förteckning över förekommande begrepp finns i formuläret för klassning)

- Vilken typ av personuppgifter som förekommer, t ex namn, adress, personnummer etc
- Om det förekommer känsliga personuppgifter och vilka dessa i så fall är
- Om det förekommer extra skyddsvärda personuppgifter och vilka dessa i så fall är

Steg 1:4 Värdera informationsmängder

Varje informationsmängd i processen ska informationsklassas i enlighet med stadens Göta Lejons anpassade klassningsmodell som finns i informationsklassningsmallen under fliken ”Klassningsmodell”.

Informationsklassningens syfte är att identifiera hur allvarliga konsekvenser som uppstår om informationssäkerheten brister i aspekterna konfidentialitet, riktighet och tillgänglighet. Informationsklassningen är tillsammans med riskanalyser de viktigaste underlagen för att i ett senare skede fatta beslut om tillräckliga säkerhetsåtgärder för att skydda informationen.

Bortse från sådan information som felaktigt hanteras i processen. Om sådan information hanteras sker återkommande bör detta tas med i kommande riskanalys.

Alla informationsmängder ska klassas på en skala mellan 0-4 för konfidentialitet, riktighet och tillgänglighet. I praktiken är det sällsynt att en informationsmängd klassas på den högsta eller lägsta nivån. Nivå 0 innebär att inget skydd behövs för den givna informationsmängden, detta kan vara aktuellt för konfidentialitet om informationen ska publiceras öppet på exempelvis en webbplats. Nivå 4 innebär information som är av vikt för *Sveriges säkerhet* och ska därför hanteras i enlighet med säkerhetsskyddslagen.

Stadens definition av begreppen konfidentialitet, riktighet och tillgänglighet är:

Begrepp	Förklaring
Konfidentialitet	Att information inte tillgängliggörs eller avslöjas för obehöriga.
Riktighet	Att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
Tillgänglighet	Att information är tillgänglig och användbar när den behövs.

En informationsmängd ska informationsklassas utifrån det värde informationen har för verksamheten. Det innebär att eventuella säkerhetsåtgärder som har vidtagits för att skydda informationen inte ska påverka informationsklassningen.

Inkommen kunddata ska som utgångspunkt klassas som konfidentialitet nivå 3 om inte annat överenskommits eller framgår av kundens egen klassning. Detta avser all information som skickas till Göta Lejon via bifogade filer, uppdatering direkt i system eller anges via mail.

Steg 1:5 Identifiera informationsbärare och leverantörer

För varje informationsmängd ska en eller flera informationsbärare identifieras. En informationsbärare är det medium som informationen överförs med eller behandlas och lagras på. Vanligen är detta en applikation eller lagringsyta, men det kan också vara via telefon eller på annat sätt. I vissa fall finns det flera informationsbärare för samma informationsmängd, exempelvis kan ett ärende inkomma via brev, e-post, telefonsamtal eller muntligen.

Informationsmängden får genom detta ett antal beroenden till en eller flera informationsbärare. Informationsklassningen av informationsmängderna är genom detta ett sätt att ställa informationssäkerhetskrav på tjänster, applikationer och infrastruktur.

För tekniska informationsbärare behöver beroende inte anges på lägre nivå än applikationsnivå. Det är alltså inte nödvändigt att ange de tekniska komponenter en applikation stödjer sig på så som databaser, nätverkskomponenter, serverhallar etc. I de fall den tekniska informationsbäraren är något annat än applikation ska detta dock anges. Det kan handla om USB-minnen, lagringsytor etc.

Identifiera leverantörer

För varje enskild informationsbärare ska en leverantör identifieras. Syfte är att veta vem kraven på säkerhetsåtgärder ska riktas mot. I de flesta fall är leverantören Intraservice eller en privat leverantör av IT-lösningar, men i vissa fall kan leverantören vara en annan nämnd eller en statlig myndighet. Det är alltid närmsta nivå i leverantörsledet som ska anges, i de flesta fall en tjänst på Intraservice. Om oklarhet råder anges endast Intraservice som leverantör.

Tillhandahålls lösningen on-prem (installerat i Göta Lejons miljö) faller en större del av säkerhetsåtgärderna på Göta Lejon, än om lösningen levereras som en SaaS-lösning (installation driftad och omhändertagen av leverantör).

Fastställ informationsklassning

Vd ska efter genomförd workshop fastställa informationsklassningen. När informationsklassningen är fastställd betraktas den som klar.

Fastställ tidpunkt för revidering

I samband med att informationsägaren fastställer informationsklassningen ska en tidpunkt för revidering av informationsklassningen fastställas. Informationsklassning ska revideras minst vart fjärde år. Detta bör noteras i bolagets verksamhetsplanering eller liknande. Vid en revidering går deltagarna igenom tidigare informationsklassning och identifierar om några förändringar har skett.

Dokumentation och kommunikation

Efter fastställning av informationsklassning ska excelarket med klassningen diarieföras i Göta Lejons diarie.

Följande handlingar ska diarieföras

- Excelfil där ni genomfört informationsklassningen
- En bild över processen som informationsklassats, om detta finns

När informationsklassningen och närliggande aktiviteter är genomförda och registrerade i diariet kan ärendet avslutas.

Informera berörda

Innebörden av informationsklassningen ska delges till berörda parter, både internt och externt, tillsammans med vilka hanteringsregler som gäller för informationen. Informationsägare ansvarar för att adressera eventuella problem med hantering i enlighet med ställda krav. Problemställningar ska lyftas med bolagets riskkommitté, säkerhetschef och IT-strateg.

Nästa steg

Efter att informationsklassningen är färdigställd används klassningsresultatet som grund för kravställning av säkerhetsåtgärder som behöver finnas kopplat till klassningsobjektet. Därefter behöver en självvärdering göras för att kartlägga vilka åtgärder som finns och vilka som behöver implementeras eller förbättras. Bedömningen och åtgärderna blir sedan ett ingångsvärde i den riskanalys som genomförs för klassningsobjektet där hot och sårbarheter ska identifieras. Är klassningsresultatet väldigt lågt kan det däremot räcka med att enbart utgå från grundkravställningen.

När riskanalysen är genomförd kan åtgärder prioriteras och en handlingsplan skapas. I vissa fall kan även mer specifika åtgärder behöva inkluderas kopplat till användningen och specifika risker som identifierats.