Instruktion för informationsklassning

1.1 Syfte

Informationsklassning handlar om att säkerhetsklassa information. Till hjälp av detta har bolaget en informationsklassningsmodell som bedömer konsekvenser av att information brister i säkerhetsaspekterna *Konfidentialitet, Riktighet och Tillgänglighet*. Personuppgiftshanteringen klassas alltid i säkerhetsaspekten Konfidentialitet.

Konsekvenserna är uppdelade i en skala 0 – 3, där 0 innebär ingen konsekvens medan 3 innebär den högsta konsekvensen då en händelse realiseras.

Denna instruktion har till syfte att beskriva hur personuppgifter skall klassas enligt bolagets informationsklassningsmodell. Genom en gemensam instruktion för hantering kan Försäkrings AB Göta Lejon upprätthålla en enhetlig och effektiv metod för att informationsklassa system/register där personuppgifter förekommer.

Instruktionen hjälper endast till att se på vilken säkerhetsklassning olika system/register ska ha med hänsyn till personuppgifterna som hanteras i det.

Notera även förhållandet till annan information: Om ett system t.ex. innehåller personuppgifter som motiverar en K1-klassificering, kan det fortfarande finnas annan information (t.ex. affärskritisk information) i systemet som gör att en högre klassificering ska göras.

Instruktionen riktar sig till samtliga medarbetare på bolaget med fokus på de roller som kan komma i kontakt med informationsklassning, dataskyddskontakt samt informationssäkerhetsansvarig.

1.2 Upplägg

Denna instruktion är upplagd som en steg för steg-instruktion där svaret på respektive fråga hänvisar dig vidare till nästa steg. Om det vid ett steg anges att ingen ytterligare aktivitet krävs behöver efterföljande frågeställningar inte besvaras. Se förenklad bild över tillvägagångssätt i figur 1 på nästa sida.

1.3 Utförande roller

Följande roller är primära utförare:

- Medarbetare
- Dataskyddsombud
- Registeransvarig,

1.4 Stödjande dokument

Se informationsklassningsmodellen nedan:

		Säkerhetsaspekt	Hanteringsregler
Konsekvensnivå		**Konfidentialitet**	Att informationstillgångar är tillgängliga endast för behöriga.
	3. Allvarlig/stor	***Konfidentiell information*** **[K3]** - Personuppgifter där förlust av konfidentialitet medför allvarlig/stor negativ påverkan på individens integritet. **Vägledning** **Mycket restriktiv hantering av informationen till en begränsad mängd individer med specifikt behov.** *Exempel är lagöverträdelser samt s.k. särskilda kategorier av personuppgifter (uppgifter om hälsa, facklig tillhörighet, m.m.)*	**Skapa:** Ange informationsklassen ”K3 - KONFIDENTIELLT” i sidhuvudet eller på därför avsett ställe. Säkerställ att märkningen framgår på varje sida. **Förvara:** Inlåst i ändamålsenligt skyddat utrymme t ex kassaskåp och endast åtkomlig för behöriga. Utskrifter ska hållas under omedelbar uppsikt. Ej tillåtet att förvara utanför ordinarie arbetsplats i pappersform. Förvaring i digitalt format kräver behörighetskontroll och stark kryptering. **Samtala:** Får endast diskuteras enskilt med personer som har behörighet att ta del av informationen. Ej tillåtet att diskutera i närvaro av obehöriga. **Distribuera:** Får under inga omständigheter spridas internt/externt utan speciella skyddsåtgärder. Informationen får endast i undantagsfall distribueras externt i pappersform. Då ska dokumentets konfiedentiallitet garanteras genom lämpligt skydd och mottagandet kvitteras av behörig person. Digital överföring endast via starkt krypterad förbindelse. Överföring via fax är ej tillåtet. **E-posta:** Internt skall informationen krypteras och mottagaren ska verifieras. Ej tillåtet att skicka till extern part om inte avtal som reglerar konfidentialliteten finns. Om avtal finns får informationen endast skickas via starkt krypterad förbindelse.

			Kasta: Pappersutskrifter makuleras i papperstugg. Digital information skrivs över med hjälp av speciellt program.
	2. Betydande/medel	***Begränsad intern information*** **[K2]** - Personuppgifter där förlust av konfidentialitet medför betydande/medelstor negativ påverkan på individens integritet. **Vägledning** **Får endast vara tillgänglig för individer som har behörighet att hantera informationen.**	**Skapa:** Ange informationsklassen ”K2 – Begränsad intern” i sidhuvudet eller på därför avsett ställe. **Förvara:** Inlåst i ändamålsenligt utrymme t ex låst arbetsrum eller dokumentskåp och endast vara åtkomlig för behöriga. Utskrifter ska hållas under uppsikt. Förvaring i digtialt format kräver behörighetskontroll. **Samtala:** Får endast diskuteras med personer som har behörighet att ta del av informationen. **Distribuera:** Får distribueras till behörig personal inom bolaget. Om informationen skickas externt ska dokumentets konfiedentiallitet garanteras. Vid

		Exempel är lön, kontonummer, uppgifter om privatliv, GPS-koordinater	överföring via fax ska mottagningen verifieras. Kryptering ska användas för digital överföring. **E-posta:** Får skickas via e-post till behörig personal inom bolaget Ej lämpligt att skicka till extern part om inte avtal som reglerar konfidentialliteten finns. Om informationen skickas externt skall det vara via krypterad förbindelse. **Kasta:** Pappersutskrifter kastas i slutna behållare/säkerhetskärl. Digital information kastas i ”papperskorgen” på datorskrivbordet, och ”papperskorgen” töms därefter direkt.
	1. Försumbar/ låg	***Öppen intern information*** **[K1]** - Personuppgifter där förlust av konfidentialitet medför försumbar/låg påverkan på individens integritet. **Vägledning** **Får hanteras av samtliga medarbetare inom Försäkrings AB Göta Lejon.** *Exempel är namn, typ av relation till Försäkrings AB Göta Lejon, kontaktuppgifter*	**Skapa:** Ange informationsklassen ”K1 – Öppen intern” i sidhuvudet eller på därför avsett ställe. **Förvara:** Inga restriktioner om informationen förvaras på ordinarie arbetsplats. Om informationen förvaras utanför ordinarie arbetsplats skall den vara under uppsikt. **Samtala:** Tillåtet att diskutera internt inom bolaget och externt till kontrollerad behörig part. **Distribuera:** Får distribueras internt inom bolaget och externt till kontrollerad behörig part. **E-posta:** Får skickas via e-post internt inom bolaget utan restriktioner. Om informationen skickas externt bör den krypteras. **Kasta:**

			Pappersutskrifter kastas i slutna behållare. Digital information kastas i ”papperskorgen” på datorskrivbordet.
	0. Ingen	***Öppen information*** **[K0]** – Offentlig information där det inte föreligger några krav på konfidentialitet ***OBS: Personuppgifter kan endast undantagsvis klassas som K0!*** *Exempel är information som till sin natur är menat att vara offentlig/spridas fritt, t.ex. personuppgifter i årsredovisning, reklamutskick, m.m.*	**Skapa:** Inga restriktioner **Förvara:** Inga restriktioner **Samtala:** Inga restriktioner. **Distribuera:** Inga restriktioner. **E-posta:** Inga restriktioner. **Kasta:** Inga restriktioner.

1. Instruktion

Besvara följande för att framgångsrikt kunna klassa personuppgifterna.

1) Innehåller systemet/register personuppgifter som utgör särskilda kategorier av personuppgifter eller är särskilt integritetskänsliga?

Kommentar: Särskilda kategorier av personuppgifter är alla uppgifter som går att koppla till en enskild fysisk levande individ och som avslöjar denna individs

a) ras eller etniskt ursprung,
b) politiska åsikter,
c) religiös eller filosofisk övertygelse,
d) medlemskap i fackförening,
e) hälsa
f) sexualliv eller sexuella läggning
g) genetiska uppgifter
h) biometriska uppgifter för att entydligt identifiera denne

Särskilt integritetskänsliga personuppgifter är de personuppgifter som rör

i) *Fällande domar i brottmål, lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder.*

Nästa steg	
Om svaret är ja	Systemet/register ska klassas som K3. *Kommentar: Om endast enstaka uppgifter förekommer kan det finnas skäl till att sänka klassningen.*
Om svaret är nej	Gå vidare till fråga 2)

2) Innerhåller system/register personuppgifter som på något sätt kan ses som integritetskänsliga?

Kommentar: Vad som är integritetskänsliga uppgifter beror ofta på sammanhange, uppgifter som generellt brukar ses som integritetskänsliga är dock

a) ekonomiska uppgifter, så som utmätning utav lön, skulder hos kronofogden, möjligen även löneuppgifter
b) värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
c) GPS-koordinater, rörelsemönster
d) information som rör någons privata sfär (särskilt uppgifter om barn)

uppgifter om sociala förhållanden

Nästa steg	
Om svaret är ja	Om inte någon annan information finns som motiverar en högre säkerhetsklassning ska system/register klassas som K2.
Om svaret är nej	Gå vidare till fråga 3).

3) Innehåller system/register övriga typer utav personuppgifter?

Kommentar: Tänk på att personuppgifter har en väldigt bred definition och är all typ av information som går att koppla till en enskild fysisk, levande individ. Vanliga exempel på detta är t.ex.

a) för-/efternamn
b) kontaktuppgifter
c) relation till Försäkring AB Göta Lejon *(kund, företagskund, medarbetare, etc)*
d) befattning och tjänsteort som medarbetare hos bolaget

Tänk även här på att sammanhang spelar stor roll vad gäller uppgifternas känslighet; te.x. är kontaktuppgifter i normalfallet tämligen harmlösa uppgifter, medan det för en person med skyddad identitet är ytterst integritetskänsliga uppgifter som bör har högsta säkerhetsklassning.

Nästa steg	
Om svaret är ja	Om inte någon annan information finns som motiverar en högre säkerhetsklassning ska system/register klassas som K1
Om svaret är nej	Om inte någon annan information finns som motiverar en högre säkerhetsklassning ska system/register klassas som K0.