VÄSTRA GÖTALANDSREGIONEN

Koncernkontoret
Enhet säkerhet

Dokumenttyp	Övergripande dokument	Version
Rutin	Riktlinjer för informationssäkerhet	1.0
Dokumentansvarig	Kontaktperson	Dnr
Valter Lindström	Monika Göransson	RS 129-2015
Beslutad av	Giltig från	Ersätter
Valter Lindström, koncernsäkerhetschef	2015-11-09	

RUTIN
FÖR
KLASSIFICERING AV INFORMATION

Mål

All information och övriga informationssäkerhetstillgångar ska vara kopplade till en ägarföreträdare, som har ansvar för att informationen och resurserna klassificeras och skyddas på rätt sätt.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

Utgångspunkt

Informationssäkerhetsarbetet ska ske utifrån generella säkerhetskrav (informationssäkerhetspolicy och riktlinjer) och de specifika säkerhetskrav som ställs av verksamheten genom informationsklassificering.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

1 Omfattning

Anvisningen gäller för hantering av organisationens information oavsett var och i vilken form hanteringen sker.

2 Beskrivning

Grunden i informationssäkerhetsarbetet är att genomföra informationsklassificering. Denna ska ta sin utgångspunkt i verksamhetsprocessen och är en form av verksamhetsanalys, som visar vilket värde informationen har för verksamheten och vilka krav som ställs på att informationen är tillgänglig, riktig, insynsskyddad och spårbar. Klassificeringen som fås fram är ett underlag som ligger till grund för fortsatt arbete med krav på IT-säkerhet, fysiskt skydd och hanteringsrutiner.

2.1 Genomförande

Informationsklassificering

- Inled arbetet med att definiera informationsobjektet/informationstyp.
  - Bedöm om informationsobjektet är en upprättad allmän handling och därmed faller under Offentlighets- och sekretesslagen.
  - I vissa fall går det inte att tydligt definiera informationsobjektet som en ”handling”. I dessa fall bedöms vilken informationstyp (person-, patient-, ekonomisk-, administrativ information osv) som ska informationsklassificeras.
- Identifiera vilka verksamheter, alternativt vilka processer som informationsobjektet/informationstypen ingår i.
- Identifiera vilka lagstiftningar som är tillämpliga för verksamheten/processen.
- Samla en grupp människor som är insatta och bekanta med verksamheten/processen och genomför informationsklassificering.
- Bedöm kraven på tillgänglighet, riktighet, konfidentialitet och spårbarhet. Ett stöd för bedömningen är de frågor som finns under exempelmatrisen, se punkt 3.
- Konsekvensbedömning sker med stöd av matris, se punkt 5.

3 Exempelmatris

Bilden nedan är ett exempel på en informationsklassificering för ett upphandlingsunderlag innan det har offentliggjorts.

	Medborgare/medarbetare	Verksamhet/Process	Ekonomi	Medborgare/medarbetare	Verksamhet/Process	Ekonomi	Medborgare/medarbetare	Verksamhet/Process	Ekonomi	Medborgare/medarbetare	Verksamhet/Process	Ekonomi
Informationssäkerhetsbegrepp Konsekvens	Tillgänglighet			Riktighet			Konfidentialitet			Spårbarhet		
Klass 1 Försumbar	x		X									x
Klass 2 Lindrig		x			x	x				x	x	
Klass 3 Allvarlig				x			x	x	x			
Klass 4 Mycket allvarlig												

Exempel:
Ett upphandlingsunderlag för mammografi innan det har offentliggjorts klassificeras enligt följande: **T2, R3, K3, S2**

4 Följande frågor är ett stöd vid informationsklassificering:

Tillgänglighet

Vilken konsekvens får det om informationen inte alls kan användas på grund av bortfall av tillgänglighet?
Vilken konsekvens får det om informationen kan användas, men endast i begränsad utsträckning?

Riktighet

Vad blir konsekvensen om obehörig person eller process förändrar informationen?
Vad blir konsekvensen om verksamheten inte upptäcker detta?

Konfidentialitet

Vad blir konsekvensen om obehörig får tillgång till informationen?
Vad händer om media får tillgång till informationen?

Spårbarhet

Vilken konsekvens får det om man inte i efterhand kan konstatera vad som hänt vid en attack mot informationstillgången?
Vilken konsekvens får det om händelser kopplade till informationstillgången inte kan härledas till en specifik användare eller process vid utredningen?

5 *Konsekvens – bedömningsmatris*

Konsekvens				
1	Försumbar	**Patient/medarbetare**	Liten påverkan på liv, hälsa, rättigheter.	Ingen eller obetydlig skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om den inträffar. Ingen eller obetydlig förtroendeskada för verksamheten.
		Process	Liten negativ effekt på verksamhetens förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.	
		Ekonomi	Ingen märkbar skadekostnad för verksamheten.	
2	Lindrig	**Patient/medarbetare**	Påverkan på liv, hälsa, rättigheter.	Begränsad skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om den inträffar. (Kan hanteras i det löpande arbetet.) Begränsad förtroendeskada för verksamheten.
		Process	Begränsad negativ effekt på verksamhetens förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.	
		Ekonomi	Viss skadekostnad för verksamheten.	
3	Allvarlig	**Patient/medarbetare**	Stor påverkan på liv, hälsa, rättigheter.	Allvarlig skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om den inträffar. Allvarlig förtroendeskada för verksamheten.
		Process	Stor negativ effekt på verksamhetens förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.	
		Ekonomi	Stor skadekostnad för verksamheten.	
4	Mycket allvarlig	**Patient/medarbetare**	Mycket stor påverkan på liv, hälsa, rättigheter (skadade eller dödsfall).	Mycket allvarlig skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om den inträffar. Mycket allvarlig förtroendeskada för verksamheten.
		Process	Mycket stor negativ effekt på verksamhetens förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.	
		Ekonomi	Mycket stor skadekostnad för verk-samheten.	

6 Funktionella säkerhetskrav

KLASS 1	INSYNSSKYDD	SPÅRBARHET	TILLGÄNGLIGHET	RIKTIGHET
Informationens skyddsbehov	*Ej känslig information*	*Inga krav på spårbarhet*	*Informationen bör finnas tillgänglig inom ett par dagar*	*Inget behov av att verifiera riktigheten i informationen*
Funktionella säkerhetskrav	Inget teknikstöd för insynsskydd	Ingen teknik för spårbarhet	Ingen teknik för redundans.	Ingen teknik eller rutiner för att kontrollera riktigheten
KLASS 2	**INSYNSSKYDD**	**SPÅRBARHET**	**TILLGÄNGLIGHET**	**RIKTIGHET**
Informationens skyddsbehov	*Skyddsvärd information med behov av begränsad åtkomst (t ex sekretessbelagd information)*	*Behov av spårbarhet, t ex kvalitetssäkring, statistik, versionshantering etc*	*Informationen bör finnas tillgänglig på dagtid inom ett antal timmar*	*Riktigheten skall kontrolleras med visst intervall*
Funktionella säkerhetskrav	Teknkstöd för insynsskydd	Teknikstöd för att uppnå spårbarhet.	Krav på viss teknisk redundans och support. Eventuellt behov av jour och beredskap	Informationens riktighet ska skyddas mot förändring, så att det inte förvanskas vid överföring.
KLASS 3	**INSYNSSKYDD**	**SPÅRBARHET**	**TILLGÄNGLIGHET**	**RIKTIGHET**
Informationens skyddsbehov	*Skyddsvärd information av högre känslighet (t ex sekretessbelagd personinformation)*	*Spårbarhet krävs för att kunna styrka en hög tillförlitlighet, bevisning etc.*	*Informationen ska finnas tillgänglig inom två timmar*	*Riktigheten ska kontrolleras för kritiska informationsobjekt*
Funktionella säkerhetskrav	Teknik och rutiner som sammantaget ger ett högt insynsskydd, t ex stark autentisering och kryptering	Teknikstöd för att uppnå spårbarhet samt rutiner för granskning av loggar.	Krav på teknisk redundans och support, krav på jour eller beredskap	Kontrolleras genom kvittens eller annan automatik per informationsobjekt. Exvis personuppgifter kontrolleras mot befolkningsregistret.
KLASS 4	**INSYNSSKYDD**	**SPÅRBARHET**	**TILLGÄNGLIGHET**	**RIKTIGHET**
Informationens skyddsbehov	*Information med mycket högt skyddsvärde, t ex säkerhetsskyddsklassad information*	Spårbarhet på individ- och systemnivå	*Informationen ska finnas tillgänglig inom 15 minuter*	Riktigheten för varje informationsobjekt ska kontrolleras och verifieras
Funktionella säkerhetskrav	Teknik och rutiner som uppfyller kraven på skydd för information för rikets säkerhet	Etablerad teknik för att uppnå spårbarhet på individnivå och systemnivå	Krav på teknisk redundans och support, krav på jour eller beredskap. Alternativa IS/IT-tjänster som kan ersätta ett bortfall 24 h övervakning av IS/IT-tjänsten	Krav på teknik för oavvislighet