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 SÄKERHETSDEKLARATION

Mål

All information och övriga informationstillgångar 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 (Säkerhetspolicy och Riktlinjer för informationssäkerhet) och de specifika säkerhetskrav som ställs av verksamheten genom informationsklassificering.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

1 Säkerhetsdeklaration av IS/IT-tjänster

Säkerhetsdeklaration ska användas då det är svårigheter att genomföra traditionell informationsklassificering. Exempelvis när vi inte vet för vilken information och i vilka situationer som IS/IT-stödet kommer att användas.

Säkerhetsdeklarationen är ett stöd för objektledaren/objektägaren i ansvaret att upprätta regler för aktuell IS/IT-tjänst samt identifiera behov av tekniska skyddsåtgärder.

Reglerna ska vara ett stöd för att förstå vilken information som är tillåten/lämplig att hantera i den aktuella IS/IT-tjänsten och på vilket sätt.

2 Genomförande

1. Skapa en översiktlig bild av IS/IT-tjänstens funktionalitet. Utgå från hur denna är möjlig att använda i verksamheten.
2. Identifiera vilka tekniska skyddsåtgärder (stark autentisering, kryptering, loggning, backup mm) som IS/IT-tjänsten tillgodoser.
3. Bedöm, utifrån verksamhetens karaktär och informationstyp, vilka lagkrav som uppfylls av IS/IT-tjänsten *(se matris bilaga 1).* Fokusera på
    a. Konfidentialitet – krav på skyddad kommunikation, stark autentisering osv
    b. Spårbarhet – signering, loggning osv
4. Bedöm IS/IT-tjänstens förmåga att tillgodose verksamhetens krav på tillgänglighet och riktighet *(se matris bilaga 1).*
    a. Tillgänglighet – finns teknisk redundans, SLA-avtal med driftorganisationen, helpdesk osv
    b. Riktighet – finns tekniska kontroller för riktighet osv.
5. Skapa regler för användning av IS/IT-tjänsten.
6. Dokumentera enligt mall, bilaga 2.
7. Deklarationen fastställs av objektägare verksamhet och IT.
8. Resultatet förs in i den samlade dokumentationen för IS/IT-tjänsten och kommuniceras på lämpligt sätt till användaren.

Funktionella säkerhetskrav *BILAGA 1*

För utförligare information om funktionella säkerhetskrav vid bedömning av IS/IT-tjänster, se Västra Götalandsregionens regelverk för informationssäkerhet.

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

BILAGA 2

SÄKERHETSDEKLARATION – [IS/IT-tjänst]		
System	**Funktioner**	**Objektfamilj**
Objektägare	**Datum för värdering**	**Värdering genomförd av**

IS/IT-tjänsten uppfyller följande säkerhetsklassificering

Konfidentialitet	**Spårbarhet**	**Tillgänglighet**	**Riktighet**
[Anges 1-4 enligt matris]			
[förklarande text, exempelvis kryptering]	[förklarande text, exempelvis loggning]	[förklarande text, exempelvis redundans]	[förklarande text, exempelvis verifiering]

Objektägaren Verksamhet företräder informationsägare och ansvarar för att upprätta och kommunicera regler för användning av IS/IT-tjänsten.

Regler för användning av tjänsten

- xxxx

Utvecklingsförslag (vid behov)

- xxxx

Ovanstående deklaration fastställs 20XX-XX-XX

.....	.....
[namnförtydligande]	[namnförtydligande]
Objektägare verksamhet	Objektägare IT