

IT-stöd för informationssäkerhetsanalys i Region Sörmland

2021-04-14



REGION
SÖRMLAND

Lite om oss

Vem är jag

Ann-Mari Nilsson

Informationssäkerhetsenheten Region Sörmland

Har tidigare jobbat med informationssäkerhet på IKEA,
Nyköpings kommun och Migrationsverket

Vad gör Informationssäkerhetsenheten

Två medarbetare

Ger stöd och råd gällande informationssäkerhet



REGION
SÖRMLAND

Informationssäkerhet

Informationstillgångar

Information (kunskap eller data) eller resurs(bärare) som hanterar information som har ett värde för Regionen.

Informationssäkerhet

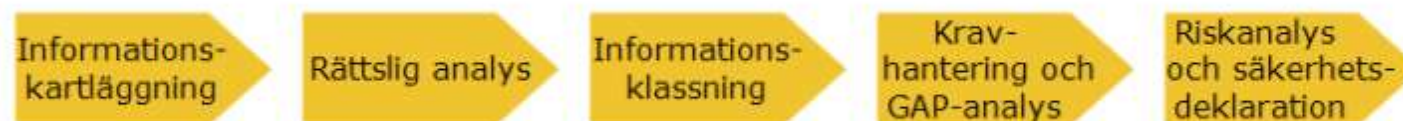
Informationssäkerhet innebär att hantera information så att

- Endast behöriga personer får ta del av den
- Den alltid går att lita på, att den är korrekt och inte är manipulerad eller förstörd
- Den alltid finns åtkomlig och användbar när den behövs

Hur säkerställs att informationen är tillräckligt säker när det finns både lagar, riktlinjer och standarder med många och olika krav på informationshanteringen?



Process för informationssäkerhetsanalys



Processen för informationssäkerhetsanalys ser till att säkerheten för regionens tillgångar omhändertas på ett enhetligt sätt.

Processen är en stödprocess.

Se till att rätt kompetenser deltar. Glöm inte bort verksamhetsspecialisterna

Informationstillgångarna är oftast objekt (IT-stöd och dess information) i förvaltning och genomförs av förvaltningen.

IT-stöd för Informationssäkerhetsanalys

ISMS står för Information Security Management System

ISMS ger stöd i att:

- Följa tillämpliga lagar
- Ta fram krav på information
- Reducera risker
- Ta fram rapporter
- Att ta fram informationssäkerhetsanalyser sker på ett enhetligt sätt och analyserna lagras på ett samlat ställe med möjlighet att överblicka hela regionens informationssäkerhetsläge.



Kartläggning av information



- Tillgångar ▾
 - Portal
 - Massuppdatering
 - Informationstillgång**
 - Personuppgiftsbeha...
- Risk >

Översikt **Detaljer** Lagar och standarder Klassificeringar Krav Beroende

Information

Namn *
Namnet på informationstillgången som är gångbart även då leverantören byts ut

Tillgångstyp *
Informationstillgång ▾

Ägare * Stöd för informationssäkerhet (1) ▾ **Ansvarig *** Ann-Mari Nilsson ▾

Generella uppgifter

Beskrivning *
Beskrivning av informationen som behandlas samt om det finns personuppgifter i informationstillgången.
Information om informationstillgångens avgränsningar.
Information om datalagring.

Livscykel *
Förvaltning och vidmakthållande ▾

Var tydlig med informationstillgångens avgränsningar. Ta förslagsvis hjälp av systemskisser

Förteckning av personuppgiftsbehandlingar

Informationskartläggning

Rättslig analys

Informationsklassning

Kravhantering och GAP-analys

Risکانalys och säkerhetsdeklaration

Översikt | Detaljer | Lagar och standarder | Klassificeringar | Krav | Beroende

Information Personuppgiftsbiträde

Information

Namn *
Administratörer av ett IT stöd eller t.ex. patientuppgifter i ett journalsystem

Tillgångstyp *
Personuppgiftsbehandling

Ägare * Stöd för informationssäkerhet (1) **Ansvarig *** Ann-Mari Nilsson

Registerförteckning personuppgiftsbehandling

Personuppgiftsansvarig nämnd/styrelse * Regionstyrelsen **Dataskyddsbud *** Namnet på Regionens dataskyddsbud

Behandlingens syfte/ändamål *
Om det handlar om administratörer kan det vara att lägga upp nya användare.
Om det avser Patienter kan det vara att utreda en sjukdomsbild.
Det kan också vara att informera elever, vårdnadshavare eller att bedriva skolmatsservering.

Vilken laglig grund för behandling används? *
Uppgift av allmänt intresse eller myndighetsutövning
Rättslig förpliktelse
Avtal
Samtycke

Vilka kategorier av registrerade? *
Invånare
Patienter
Medarbetare
Kunder

Vilka kategorier av personuppgifter behandlas? *
Personnummer
Hälsouppgifter

Vilka kategorier av mottagare? *
Andra myndigheter

Varifrån hämtas personuppgifterna? *
SCB, Eks, SPAR etc.

Tillgångar

Portal

Massuppdatering

Informationstillgång

Personuppgiftsbeha...

Risk

Krav på dataskydd enligt dataskyddsförordningen

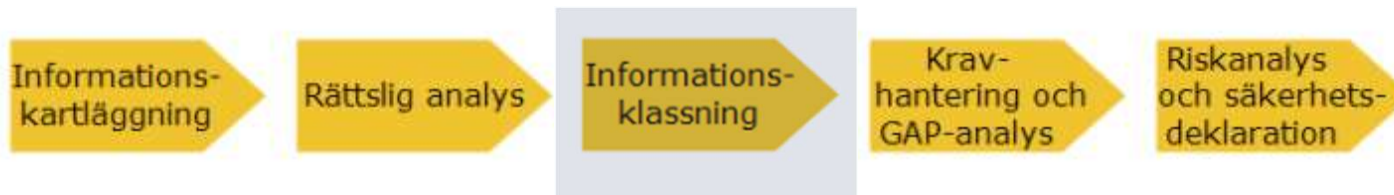
Rättslig analys



- Tillgångar ▾
 - Portal
 - Massuppdatering
 - Informationstillgång**
 - Personuppgiftsbeha...
- Risk ▸

Översikt	Detaljer	Lagar och standarder	Klassificeringar	Krav	Beroende
Namn					Nivå
Finns det information som direkt eller indirekt kan identifiera en levande person?					Ja ▾
Är Lag.(2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster tillämplig?					Nej ▾
Hanteras personuppgifter i syfte att bedriva vård eller tandvård					Nej ▾
Förekommer skyddade personuppgifter?					Nej ▾
Förekommer information som skulle kunna hota Sveriges säkerhet?					Ja ▾
Förekommer information som används för att förebygga eller beivra brott?					Nej ▾
Är Lag.(1993:584) om medicintekniska produkter tillämplig?					Nej ▾
Är Lag.(2018:597) om kommunal bokföring och redovisning tillämplig?					Ja ▾

Informationsklassning



Översikt	Detaljer	Lagar och standarder	Klassificeringar	Krav	Beroende
Namn	Nivå				
Konfidentialitet	- Välj -				
Riktighet	- Välj -				
Tillgänglighet	K0 Ringa konsekvens (ÖPPEN) K1 Måttlig konsekvens (INTERN) K2 Betydande konsekvens (KÄNSLIGT) K3 Allvarlig konsekvens (MYCKET KÄNSLIGT) K4 Synnerligen allvarlig konsekvens (HEMLIGT)				
<input type="button" value="✓ Spara"/>					

Klassa informationen utifrån sammanhang

Kravhantering och GAP-analys



Översikt | Detaljer | Lagar och standarder | Klassificeringar | **Krav** | Beroende

Urval Uppfylld

Visa krav som är automatiskt uppfyllda
 Visa uppfyllnad

+ Lägg till användarupplagda krav

[6] Organisation av informationssäkerhetsarbetet 1

Kravsektion / Krav

Inte tillämplig

→ Informationssäkerhetsincidenter som utgör personuppgiftsincidenter ska rapporteras till integritetsskyddsmyndigheten inom 72h från upptäckt

Dataskydd 3

[8] Hantering av informationstillgångar 1

Kraven är hämtade från de åtgärder som finns definierade i ISO27002

Omhänderta GAP i riskanalysen

Risikanalyt

Informations-
kartläggning

Rättslig analys

Informations-
klassning

Krav-
hantering och
GAP-analys

Risikanalyt
och säkerhets-
deklaration

Översikt Detaljer Lagar och standarder Klassificeringar Krav Beroende

Risikregister + Lägg till

▼ Riskmall	▼ Risker	▼ Åtgärder	▼ Senast gra...	
Informationssäkerhet	0	0	2021-04-13	Redigera

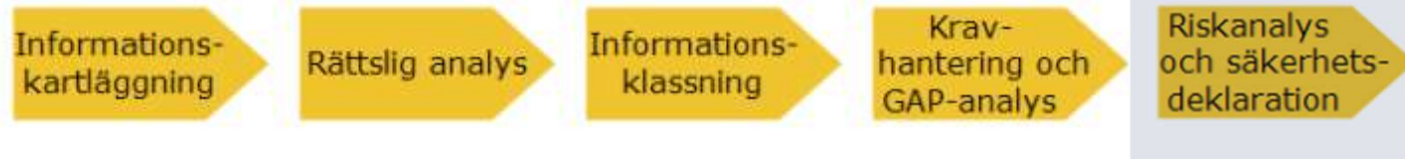
15 ▼ objekt per sida

Beroendegraf 🔍 🔍 Djup 1 ▼ Underliggande tillgångar

Ingen data tillgänglig för beroendegraf

Att identifiera risker innebär att undvika eller reducera risker genom att titta i Kristalkulan. Att vara steget före.

Riskregister



Vilka är hoten
Vilka är sårbarheterna
Vad är **skyddsvärdet**
Ta hjälp av tidigare
inträffade händelser

Översikt Medlemmar Historik Granskningscykel

Riskregister

+ Lägg till Importera risk Importera hot

▼ RiskID ▼ Risktitel ▼ Riskägare ▼ Riskvärde ▼ Senast gra... ▼ Status ▼ Prioriterad risk

Inget innehåll funnet

15 ▼ objekt per sida

Identifiering av risk



Risktitel *

Namnet på risken som tydligt beskriven en inträffad händelse

Status *

Aktiv

Riskbeskrivning

Beskrivning av den identifierade risken

Risikpåverkan

Beskrivning av hur risken drabbar

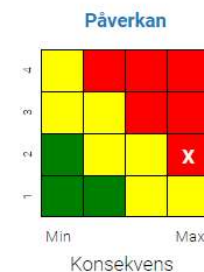
Identifieringsdatum

2021-04-13

Bedömning av risk



Sannolikhet*	<input type="text" value="2"/>	
Konsekvens		Riskvärde
Ekonomisk förlust	<input type="text" value="Obetydlig förlust"/>	<input type="text" value="2"/>
Förtroende	<input type="text" value="Måttlig påverkan"/>	<input type="text" value="4"/>
Verksamhet	<input type="text" value="Betydande påverkan"/>	<input type="text" value="6"/>
Personskada	<input type="text" value="Allvarlig påverkan"/>	<input type="text" value="8"/>
Risksumma		20



Riskåtgärder



Redigera riskförebyggande åtgärd

ÅtgärdsID

Infosäk0001-001

Status *

Aktiv

Titel *

Beskrivande titel vad som behöver göras för att begränsa riskens effekter

Beskrivning

Beskrivning av vad som behöver hanteras.

Det kan vara administrativa, tekniska eller fysiska åtgärder.

Exempel på åtgärder kan vara rutiner, implementera ett tekniskt skydd eller sätta upp ett larm.

Identifieringsdatum

2021-04-13

Åtgärdsägare *

Ann-Mari Nilsson (ann-mari.nilsson@regionsormland.se)

Förfalldatum *

2021-04-14

Kopplade risker

Infosäk0001 - Namnet på risken som tydligt beskriven en inträffad händelse

✓ Spara

✗ Avbryt

En risk kan ha flera åtgärder och en åtgärd kan reducera flera risker

En identifierad risk kan ge upphov till nya krav



REGION
SÖRMLAND

Säkerhetsdeklaration



Säkerhetsdeklarationen ger en samlad bild av informationstillgångens skydd.

Säkerställ åtgärder och efterlevnad med

- Avtal
- Internrevision
- Externrevision

När är arbetet klar

Det är när analysen är klar som arbetet börjar

- Omhändertagandet av riskerna
- Den iterativa processen

Informationssäkerhet är aldrig starkare än dess svagaste länk, fastna inte i detaljer, plocka dem lågt hängande frukterna.

Det är bättre att färdigställa en analys än att genomföra halva processen detaljerat.



IT-stöd för informationssäkerhetsanalys



En samlad plats för samtliga informationssäkerhetsanalyser ger oss en överblick av Regionens samlade säkerhetsläge.

Ger underlag för var vi behöver ge mer stöd.

Ger uppföljning och statistik att ta med till högsta ledningens årliga säkerhetsgenomgång.

