



KONFERENSEN
**INFORMATIONSSÄKERHET
FÖR OFFENTLIG SEKTOR**

14–15 SEPTEMBER 2016



Verksamhetsdriven informationssäkerhet genom informationsklassning och målgruppsanpassade riktlinjer

Per Oscarson
Informationssäkerhetsansvarig
Örebro kommun



Per Oscarson

- Informationssäkerhetsansvarig på Örebro kommun
- Medlem i SIS TK 318 (SS-ISO/IEC 27000-serien)
- Fil Dr och Fil Lic vid Linköpings universitet
- Har tidigare varit
 - CISO/CSO på Folksam
 - Informationssäkerhetsexpert på MSB
 - Informationssäkerhetskonsult på Nexus och Transcendent Group
 - Universitetslärare, Örebro universitet



- Ca 142 000 invånare (7:e största i Sverige)
- Mitt i Sveriges befolkningsmässiga centrum
- Örebro är 750 år gammal. Slottet började byggas redan på 1200-talet
- Logistikcentrum: Flyg, järnväg, Europavägar
- Örebro universitet, 16 gymnasieskolor, över 40 kommunala grundskolor och 15 friskolor



- Leds av S, KD och C
- Ca 12 000 anställda
- Ca 20 nämnder
- Tre programområden
 - Barn och utbildning
 - Samhällsbyggnad
 - Social välfärd
- Central styrning och administration i kommunstyrelseförvaltningen
- Informationssäkerhetsansvarig placerad på IT-avdelningens IT-strategienhet



Informationssäkerhet – övergripande dokumentstruktur

Underlag

Informations-
säkerhetsanalys



Motiverar

Styrande dokument

Handlingsplan
för informations-
säkerhet (årlig)

Informations-
säkerhets-
policy

Riktlinjer för
informations-
säkerhet

Instruktioner

Stödande material (exempel)

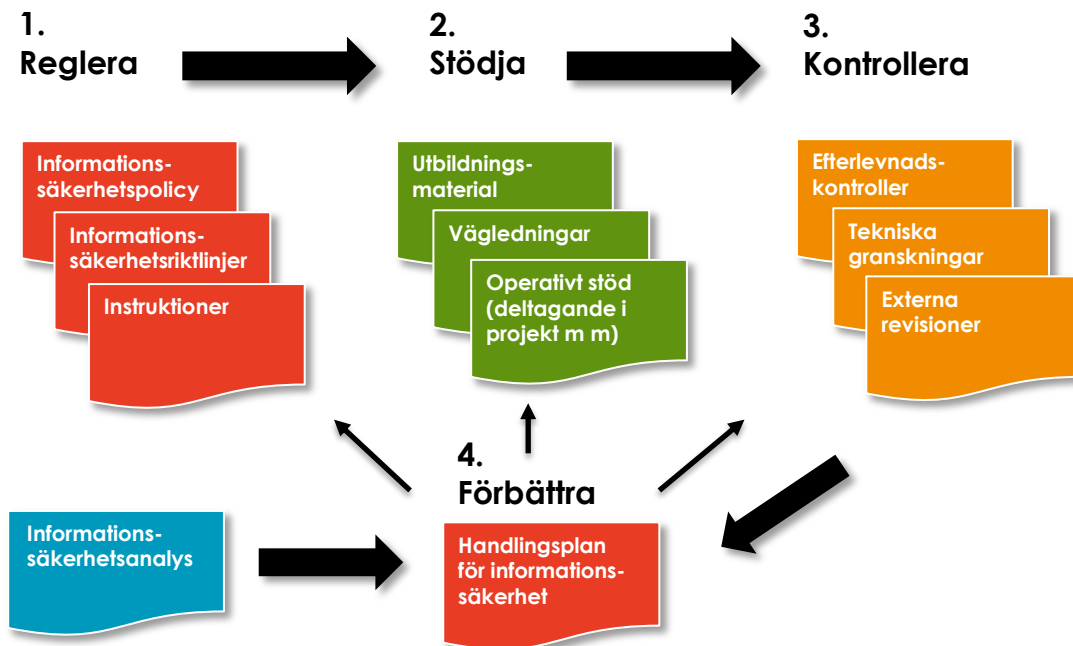
Populärfolder

Infosäk på
intranätet

E-utbildning

Vägledningar

Essensen av informationssäkerhetsstyrning



Målgruppsindelade riktlinjer

Gammal version

Riktlinjer för
informations-
säkerhet

Strukturerad
utifrån
SS-ISO/IEC
27002:2005



Ny version

Riktlinjer för
informations-
säkerhet

Målgruppsbaserad
struktur

Innehåller
relevanta delar ur
SS-ISO/IEC
27002:2014

Målgrupper/kapitel

1. Alla medarbetare

2. Styrning av
informationssäkerhet

3. Informationssäkerhet i
verksamhetsnära förvaltning

4. Informationssäkerhet
i IT-miljön

Målgruppsindelade riktlinjer

Kapitel

Innehåll

Målgrupper

Stödmaterial

(Internt och externt)

Inledning

Omfattning, struktur m.m.
Introduktion till infosäk
Dispenser

Alla medarbetare

Kapitel A Informationssäkerhet för medarbetare

Medarbetares ansvar
Informationsklasser
Åtta avsnitt utifrån DISA
(A1 – A8)

Alla medarbetare

Externa som kommer åt
informationstillgångar

E-utbildning

Intranät

Instruktioner

Kapitel B Styrning av informationssäkerhet

Övergripande organisation,
roller och ansvar
Sju avsnitt om hur
informationssäkerhet styrs i
kommunen (B1 – B7)

Roller som deltar i
infosäkarbete

Roller med verksamhets-
ansvar

Standarder

Mtrl. från MSB

Litteratur,
forskning m.m.

Kapitel C Informationssäkerhet i verksamhetsnära förvaltning

Roller och ansvar
Åtta områden inkl.
klassning av information
och objekt (C1 – C8)

Roller i verksamhetsnära
förvaltning: objektägare,
förvaltningsledare m fl.

Metoder

Vägledning

Kapitel D Informationssäkerhet i IT-miljön

Roller och ansvar
Tio avsnitt utifrån kapitel i
27002 med IT-inriktning
(D1 – D10)

Chefer och medarbetare
på IT-avdelningen

Roller i IT-nära förvaltning

Standarder

Vägledning

Instruktioner

Kravkatalog

Tydligare riktlinjer

För att underlätta efterlevnad och uppföljning har dokumentet tydliggjorts bl.a. genom att separera informativ och motiverande text och obligatoriska riktlinjer.

Riktlinjerna är i tabellform med rött tabellhuvud medan andra tabeller, figurer m.m. är i blått. Exempel:

Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person, och dessutom ha en viss längd och komplexitet. Krav på lösenord:

Riktlinjer för utformning av lösenord

- A.1.1** Lösenord ska vara minst X tecken långt, gärna längre.
- A.1.2** Lösenord ska innehålla minst en gemen, en versal och en siffra.

Tips på bra lösenord som är enkla att minnas är att tänka ut en mening. Justera sedan stora och små bokstäver och bilda lösenordet. Exempel:

Örebro kommuns modell för informationsklassning

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet
2 Höga skydds-krav	Konfidentiell information som, om den sprids till obehöriga, kan medföra allvarliga konsekvenser för Örebro kommun, externa aktörer eller individer	Information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för Örebro kommun, externa aktörer eller individer	Information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för Örebro kommun, externa aktörer eller individer
1 Normala skydds-krav	Intern information som, om den sprids till obehöriga, kan medföra måttliga negativ påverkan på Örebro kommun, externa aktörer eller individer	Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på Örebro kommun, externa aktörer eller individer	Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på Örebro kommun, externa aktörer eller individer
0 Inga skydds-krav*	Öppen information som kan spridas fritt inom och utom Örebro kommun		

***Krav finns alltid att information ska vara riktig och tillgänglig!**

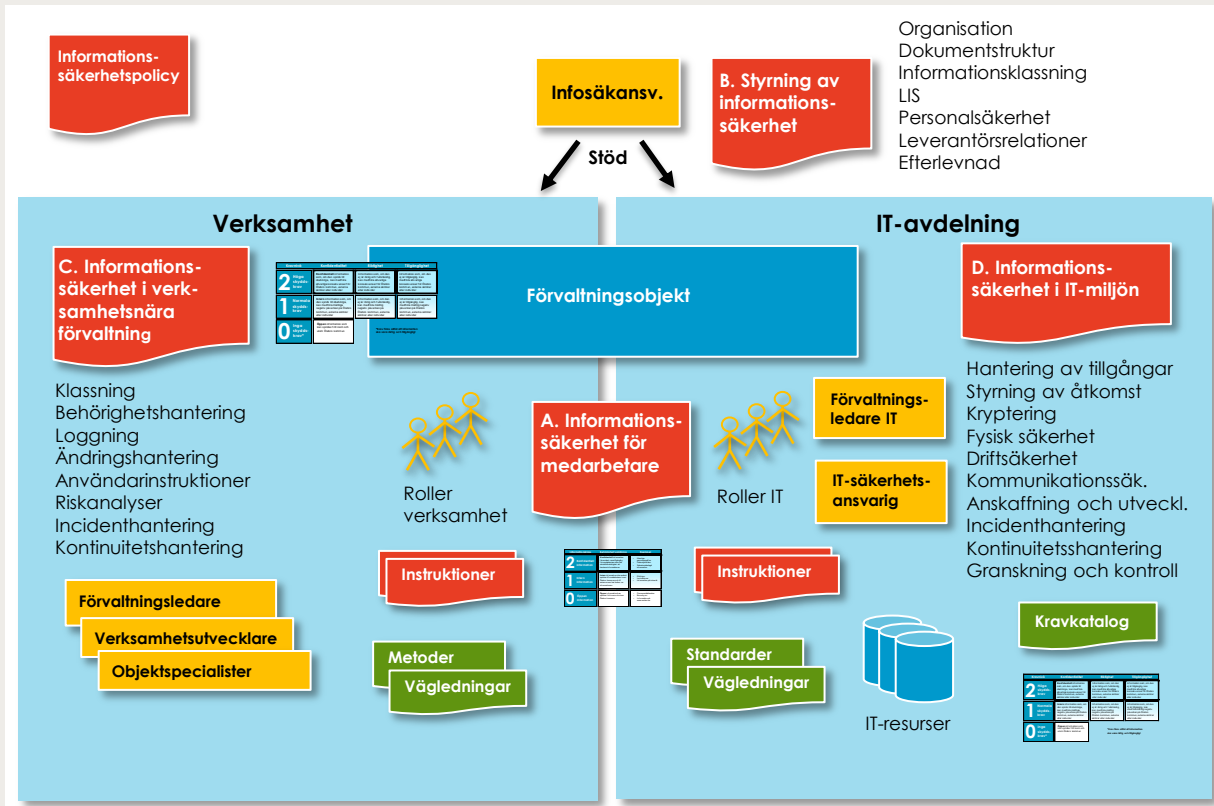
Modell för medarbetare – endast konfidentialitet

Informationsklass	Behörighet/spridning	Exempel
2 Konfidentiell information	Konfidentiell information får endast vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen	<ul style="list-style-type: none">• Känsliga personuppgifter• Patientjournaler• Sekretessbelagd information
1 Intern information	Intern information ska endast spridas till medarbetare inom Örebro kommun och till externa som har behov av informationen	<ul style="list-style-type: none">• Riktlinjer• Instruktioner• Information på intranät
0 Öppen information	Öppen information kan spridas fritt inom och utom Örebro kommun	<ul style="list-style-type: none">• Pressmeddelanden• Broschyrer• Information på www.orebro.se

Informationsklassning i riktlinjerna

- Kapitel A – Informationssäkerhet för medarbetare
 - Del av modellen: konfidentialitet
 - Särskilda hanteringsregler för konfidentiell information
- Kapitel B – Styrning av informationssäkerhet
 - Övergripande om informationsklassning
 - Klassningsmodellen
- Kapitel C – Informationssäkerhet för verksamhetsnära förvaltning
 - Riktlinjer för klassning av information och objekt
- Kapitel D – Informationssäkerhet i IT-miljön
 - Normala och höga skyddskrav på säkerhetsåtgärder gällande konfidentialitet, riktighet och tillgänglighet

Verksamhetsdriven informations säkerhet



Informationssäkerhet för offentlig sektor 2016

Frågor?

Per Oscarson

Informationssäkerhetsansvarig

Örebro kommun

per.oscarson@orebro.se