



KONFERENSEN
**INFORMATIONSSÄKERHET
FÖR OFFENTLIG SEKTOR**

14–15 SEPTEMBER 2016





Myndigheten för
samhällsskydd
och beredskap

Nya krav på systematiskt informationssäkerhets arbete

Helena Andersson

Verksamheten för cybersäkerhet
och skydd av samhällsviktig
verksamhet

Myndigheten för samhällsskydd
och beredskap

Myndigheten för samhällsskydd och
beredskaps författningssamling

Utgivare: Key Högstetam, Myndigheten för samhällsskydd och beredskap
ISSN 2004-1836

Myndigheten för samhällsskydd och beredskaps
föreskrifter¹ om statliga myndigheters
informationssäkerhet;

beslutade den 1 mars 2016.

Myndigheten för samhällsskydd och beredskap föreskriver följande med
stöd av 21 § förordningen (2015:1052) om krisberedskap och
bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Tillämpningsområde

1 § Denna författning innehåller föreskrifter som ansluter till
bestämmelserna om statliga myndigheters informationssäkerhet i 19 §
förordningen (2015:1052) om krisberedskap och bevakningsansvariga
myndigheters åtgärder vid höjd beredskap.

2 § Om det i en annan författning finns någon bestämmelse om statliga
myndigheters informationssäkerhet som avviker från denna författning,
gäller den bestämmelsen.

3 § I 19 § förordningen (2015:1052) om krisberedskap och bevaknings-
ansvariga myndigheters åtgärder vid höjd beredskap finns föreskrifter om
varje myndighets ansvar för säker informationshantering. Ansvaret gäller
även när myndighetens information hanteras av en extern aktör eller när
myndigheten tillhandahåller andra aktörer tjänster för informationshantering
inom e-förvaltning eller motsvarande.

I de fall en myndighet anlitar en annan myndighet för att fullgöra uppgifter
som regleras i denna författning ska de berörda myndigheterna tydligt
dokumentera sitt samarbete. Det ska i dokumentationen tydliggöras vilken
myndighet som är ansvarig för att uppfylla kraven som ställs i denna
författning. Informationsklassning enligt 9 § p.1 ska utföras av den
myndighet som äger informationen.

¹ Allmänna råd som ansluter till föreskrifternas finns på sid 5.



EU-reglering att beakta

- **EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/1148** av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen
 - Ska vara införlivat senast 10 maj 2018 (NIS-direktivet)
 - Ställer krav på nationell strategi, inför rapporteringskrav på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, inrättar samverkansgrupper på EU nivå, krav på identifiera leverantörer av samhällsviktiga tjänster samt att säkerställa att de vidtar ändamålsenliga säkerhetsåtgärder m m.
- **EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679** av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (Dataskyddsförordningen)
 - Börjar gälla den 25 maj 2018
 - Ex ”rätt att bli glömd”
 - Integrity by design
 - skadestånd
 - ansvarsregler



Myndigheten för
samhällsskydd
och beredskap

På nationell nivå ...

- Förslag - ny säkerhetsskyddslag
- Obligatorisk it-incidentrapportering
- Nya krav på systematiskt informationssäkerhetsarbete



Myndigheten för
samhällsskydd
och beredskap

Fokus för regelverken

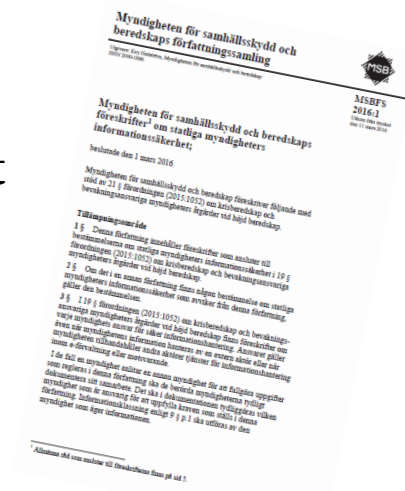
- Statliga myndigheter
- Obligatorisk it-incidentrapportering – förtydliga vad, hur och när
- Systematiskt informationssäkerhetsarbete – ledningssystem för informationssäkerhet
- Inbördes koppling
- Gäller från och med april 2016



Myndigheten för
samhällsskydd
och beredskap

Bakgrund - nya föreskrifter om statliga myndigheters informationssäkerhet

- Då gällande föreskrifter MSBFS 2009:10
- Nya versioner av standarderna
- Enkätundersökningen
- Riksrevisionen
- Analysunderlag
- Förändrade villkor/miljö
- **Föreskrifterna ska bli ett ännu bättre stöd för det praktiska arbetet!**





Myndigheten för
samhällsskydd
och beredskap

Portalparagraf 5 §

Varje myndighet ska bedriva ett **systematiskt och riskbaserat** informationssäkerhetsarbete med stöd av ett **ledningssystem** för informationssäkerhet. I detta arbete ska standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 **beaktas**.

Tillräckliga resurser ska tilldelas för informationssäkerhetsarbetet samt löpande och regelbunden information lämnas till **myndighetsledningen**.



Myndigheten för
samhällsskydd
och beredskap

Nya regler: ansvar och definitioner

- Tydliggör ansvar vid organisationsöverskridande samarbeten och outsourcing
- Definition av ledningssystem





Myndigheten för
samhällsskydd
och beredskap

Nya regler: Ledningssystemet



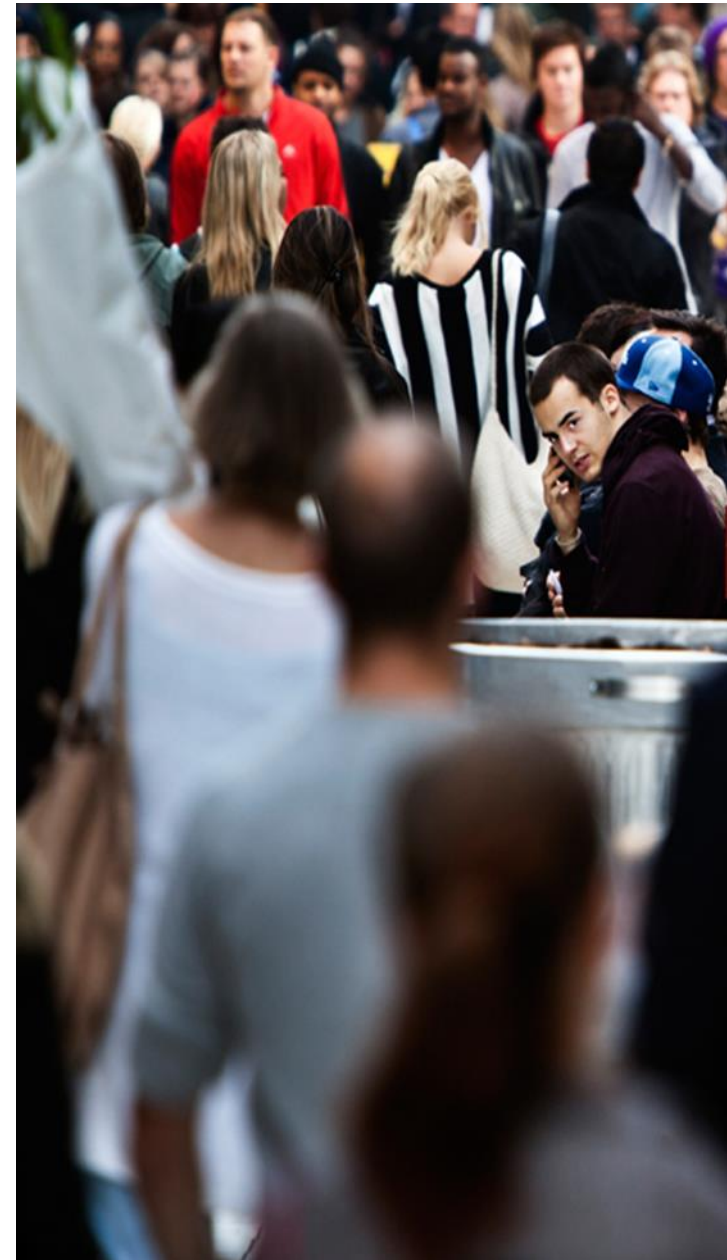
- Tydliga krav på ledningssystemets utformning
 - Verksamhetens behov
 - Styrande för all informationshantering
 - Tydliggöra ansvar
 - Tilldela befogenheter
 - Arbetet ska bedrivas samordnat
 - Regelbundet utvärderas och utvecklas (inkl extern granskning i allmänna råd)



Myndigheten för
samhällsskydd
och beredskap

Nya regler: säkerhetskultur och processarbete

- God säkerhetskultur
- Processinriktat arbete med stöd av modeller
 - informationsklassning, analysera hot och risker, identifiera åtgärder, följa upp, utveckla, dokumentera.





Myndigheten för
samhällsskydd
och beredskap

Nya regler: oönskade händelser

- Incidenthantering
- Kontinuitetshantering





Några tips

- **Samverka:** Skapa grupper med andra yrkesgrupper jurister, arkivarie, personuppgiftsombud, it-drift, nät drift, upphandling, revision, projektkontor
- **Dokumentera nuläge:** Vad har redan gjorts, bygg vidare och utveckla det
- **Draghjälp:** Dataskyddsförordningen och annan reglering kan ge stöd i argumentationen
- **Säkerhetskulturen:** Satsa på kompetenshöjning i organisationen
- **Använd föreskrifterna:** Föreskrifterna är ett koncentrat av vad som måste vara på plats
- **Nätverka:** Nyttja kompetensen i de många nätverk som finns.



Myndigheten för
samhällsskydd
och beredskap

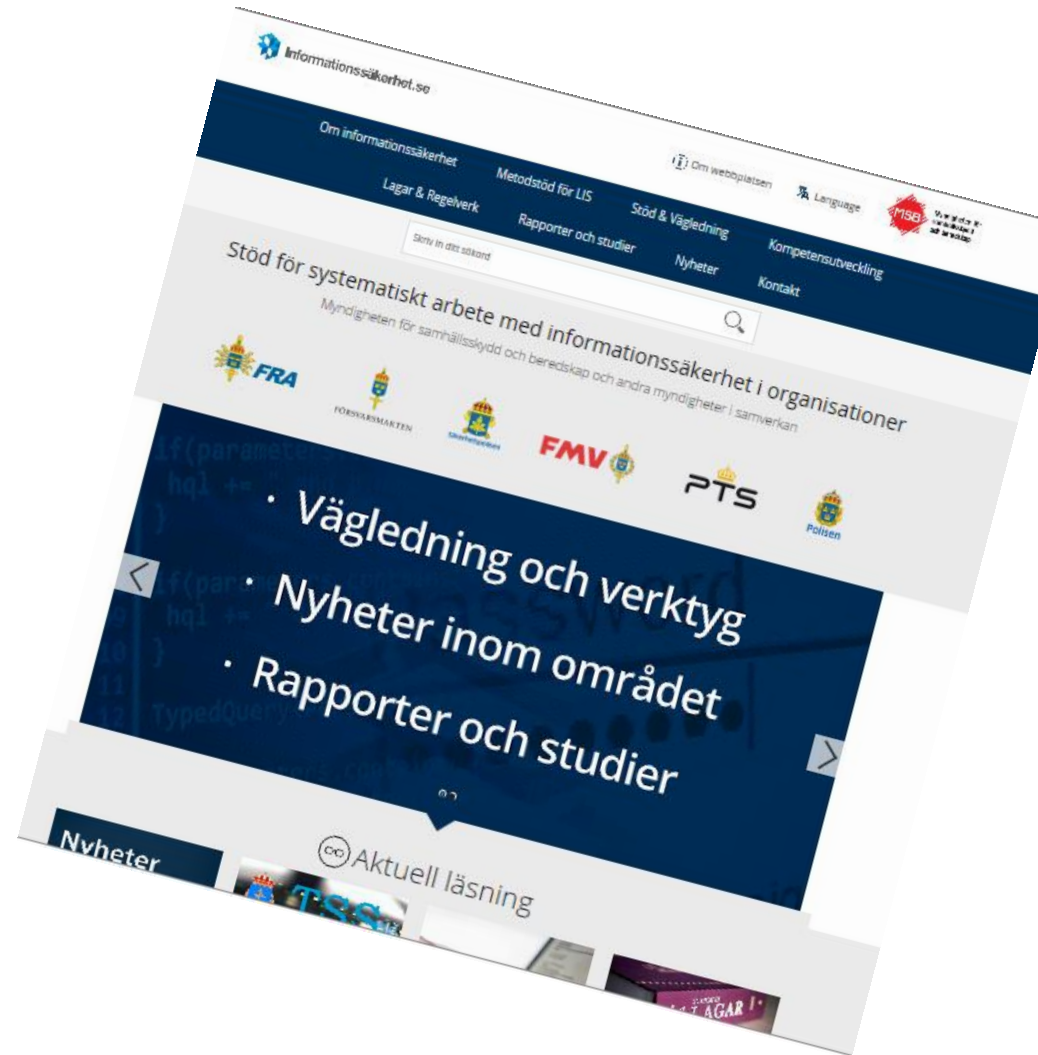
Tillgängligt stöd för arbetet

www.informationssakerhet.se

Filmer

Översyn av metodstödet

vägledningar





Myndigheten för
samhällsskydd
och beredskap

Frågor och tack!

Helena Andersson och Svante Nygren

Verksamheten för cybersäkerhet och skydd av samhällsviktig verksamhet

Helena.andersson@msb.se

Svante.nygren@msb.se