

# MSB:s föreskrifter om säker informationshantering för statliga myndigheter

- fördjupning på säkerhetsåtgärder i informationssystem i MSBFS 2020:7 – med fokus på krav på behörigheter, digitala identiteter och autentisering

# Föreskriftspaket för statliga myndigheter

- om informationssäkerhet (MSBFS 2020:6)
- om säkerhetsåtgärder i informationssystem (MSBFS 2020:7)
- om rapportering av it-incidenter (MSBFS 2020:8)



# Behörigheter, digitala identiteter och autentisering ( bild 1 av 4)

*4 kap.*

*3§ Myndigheten ska säkerställa att endast behöriga användare och informationssystem har åtkomst till it-miljön och utforma sin behörighetshantering på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver.*

Photo by Mehdi Faiz from unsplash.com

# Behörigheter, digitala identiteter och autentisering (bild 2 av 4)

*4 kap.*

*4§ Digitala identiteter som ger systemadministrativ behörighet ska endast användas för systemadministration och tilldelas restriktivt.*

Photo by Rowan Hauvel from [unsplash.com](https://unsplash.com)

# Behörigheter, digitala identiteter och autentisering (bild 3 av 4)

4 kap.

5§ Flerfaktorsautentisering ska användas vid

1. *Egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk,*
2. *Systemadministrativ åtkomst till informationssystem, och*
3. *Åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd.*

Photo by Oliur from unsplash.com

# Behörigheter, digitala identiteter och autentisering (bild 4 av 4)

*4 kap.*

*6§ Myndigheten ska ha interna regler för hantering av autentiseringsuppgifter med krav på*

- 1. Längd och komplexitet*
- 2. När byte ska ske,*
- 3. Hur distribution ska ske, och*
- 4. Hur autentiseringsuppgifter ska skyddas*

Photo by Jaz Kong from unsplash.com

# Vägledning för arbetet med säkerhetsåtgärder i informationssystem



FÖRHANDSUTGÅVA  
2020-09-01

Synpunkter ska skickas in innan 2020-10-31

Detta är en förhandsutgåva av en kommande vägledning, en så kallad "public review", och innehållet kan komma att ändras utifrån synpunkter som inkommer. Synpunkter på förhandsversionen ska skickas in innan 2020-10-31. Planerat att en fastställd version av vägledningen publiceras vid årsskiftet 2020/2021.

## Vägledning - säkerhetsåtgärder i informationssystem för statliga myndigheter



i nätverkssegment och filtrering av nätverkstrafik  
ör att förhindra spridning av incidenter, samt att upptäcka, skydda och  
genom att införa säkerhetsåtgärder mot oönskad intern och extern

FS 2020:7

ska förhindra spridning av incidenter och minska konsekvenser av  
n att placera informationssystem med olika funktioner i separata  
t i sin produktionsmiljö.

ner i produktionsmiljön bör placeras i separata nätverkssegment  
för användare.  
för administration.

stemsäkerhetsfunktioner i form av behörighetskontrollsystem,  
ggning, filtrering och liknande.  
dfunktioner i form av skrivare, scanner och liknande.  
verk.

8. Extern åtkomliga tjänster.
9. Informationssystem som sammankopplas med informationssystem hos extern aktör.
10. Industriella informations- och styrsystem.
11. System som innehåller sårbarheter som inte kan hanteras.

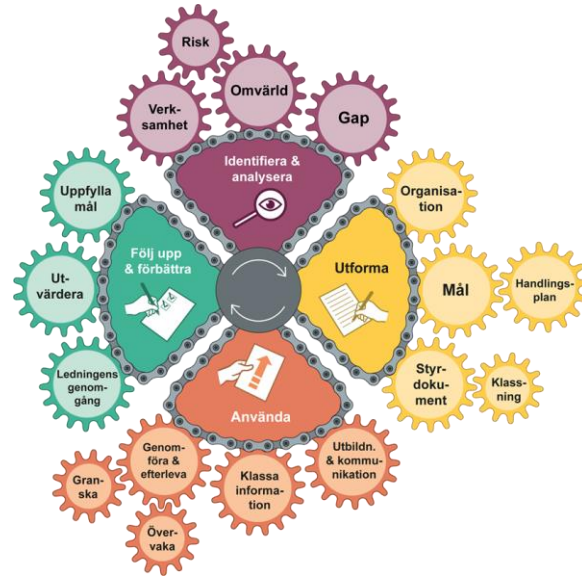
4 kap. 2 §

Myndigheten ska filtrera nätverkstrafiken så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.

- Ger bakgrund till och syfte med föreskriftskraven
- Ger stöd för vad man ska beakta när man utformar olika säkerhetsåtgärder
- Ger förslag på lösningar
- Vägledningen kommer att uppdateras regelbundet
- [www.msb.se](http://www.msb.se) och [www.informationssakerhet.se](http://www.informationssakerhet.se)

# Sammanfattning

- Ett föreskriftspaket om säker hantering av information – föreskrifter om
  - systematiskt informationssäkerhetsarbete
  - säkerhetsåtgärder i informationssystem
  - rapportering av it-incidenter
- Uppdaterat och nytt stödmaterial
- En god informationssäkerhet i organisationen bidrar till att bygga samhällets säkerhet



2020-09-04 Synpunkter ska skickas in innan 2020-10-31

Detta är en förhandsutgåva av en kommande vägledning, en så kallad "public review", och innehållet kan komma att ändras utifrån synpunkter som inkommer. Synpunkter på förhandsversionen ska skickas in innan 2020-10-31. Planerat att en fastställd version av vägledningen publiceras vid bruket 2020/2021.

Vägledning - säkerhetsåtgärder i informationssystem för statliga myndigheter



1. Uppdelning i nätverkssegment och filtrering av nätverkstrafik  
 Det är viktigt att dela upp nätverket för att förhindra spridning av incidenter, samt att typiska, styrlida och svåra organisationens nätverk genom att isolera säkerhetsåtgärder mot oönskad intern och extern trafik.

1. Koppling till MSBFS 2020:7

1.1 §  
 Myndigheten ska förhindra spridning av incidenter och minska konsekvenser av angrepp genom att placera informationssystem med olika funktioner i separata nätverkssegment i sin produktionsmiljö.

1.1 §  
 Följande funktioner i produktionsmiljön bör placeras i separata nätverkssegment:

1. Klienter för användare
2. Klienter för administration
3. Serverar
4. Centrala systemsäkerhetsfunktioner i form av beredskapskontrollsystem, säkerhetsloggning, filering och klassning
5. Centrala stöd funktioner i form av skript, scanner och klassande
6. Trådlös nätverk
7. Gästnätverk
8. Extremt inkomliga tjänster
9. Informationssystem som sammankopplas med informationssystem hos externa aktörer
10. Industriella informations- och styrsystem
11. System som innehåller skadabatter som inte kan hämtas.

Myndigheten ska filtrera nätverkstrafiken så att endast nödvändiga dataflöden förkommer mellan olika nätverkssegment.