# Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Anna Asp, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

**MSBFS 2018:8**
Utkom från trycket den 30 oktober 2018


# Myndigheten för samhällsskydd och beredskaps föreskrifter[1] om informationssäkerhet för leverantörer av samhällsviktiga tjänster;

beslutade den 23 oktober 2018.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 7 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

## Tillämpningsområde

**1 §** Denna författning innehåller bestämmelser om det systematiska och riskbaserade informationssäkerhetsarbete som leverantörer av samhällsviktiga tjänster ska bedriva enligt 11 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

**2 §** Sådant systematiskt och riskbaserat informationssäkerhetsarbete som avses i 1 § ska även omfatta den hantering av nätverk och informationssystem som utkontrakteras till en extern aktör. Innan utkontraktering ska risker för den samhällsviktiga tjänsten identifieras och hanteras. De säkerhetsåtgärder som den externa aktören ska vidta ska regleras i avtal.

## Uttryck i författningen

**3 §** De uttryck som definieras i 2 § i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster har samma innebörd i denna författning.

**4 §** I denna författning avses med

| | |
|---|---|
| *extern aktör* | Underleverantörer, inhyrda konsulter eller motsvarande. |

[1] Allmänna råd som ansluter till föreskrifterna finns på sid 5.

| | |
|---|---|
| *informationsklassning* | Att genom konsekvensanalys identifiera skyddsbehovet för en viss typ av information. |
| *informationssäkerhet* | Bevarande av konfidentialitet, riktighet och tillgänglighet hos information. |
| *ledningssystem för informationssäkerhet* | Del av leverantörens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhet. |
| *leverantör* | Leverantör av samhällsviktig tjänst enligt Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:7) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. |

**Systematiskt och riskbaserat informationssäkerhetsarbete**

**5 §** Varje leverantör ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.

Det systematiska och riskbaserade informationssäkerhetsarbetet ska utformas och samordnas utifrån organisationens behov. Det ska vara styrande avseende informationshantering i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster.

Arbetet ska dokumenteras.

**6 §** En leverantör ska utifrån identifierade risker och behov

1. tydliggöra ledningens och övriga organisationens ansvar avseende informationssäkerhetsarbetet,
2. tilldela nödvändiga resurser, mandat och befogenheter för de funktioner som arbetet med informationssäkerhet kräver, samt
3. säkerställa att informationssäkerhetsarbetet regelbundet och vid behov utvärderas och anpassas.

Arbetet ska dokumenteras.

**Närmare krav på informationssäkerhetsarbetet**

**7 §** En leverantör ska upprätta en informationssäkerhetspolicy där ledningens målsättning med och inriktning för organisationens informationssäkerhetsarbete framgår. Leverantören ska också upprätta de

interna regler och det stöd som i övrigt krävs för organisationens informationssäkerhetsarbete.

**8 §** En leverantör ska ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att

1. klassa information med utgångspunkt i vilka konsekvenser som kan uppkomma vid brister i konfidentialitet, riktighet och tillgänglighet,
2. identifiera, analysera och värdera risker för organisationens information, nätverk och informationssystem,
3. utifrån genomförd informationsklassning och riskbedömning införa ändamålsenliga och proportionella säkerhetsåtgärder,
4. följa upp och utvärdera säkerhetsåtgärder i syfte att vid behov anpassa skyddet av informationen, samt
5. fortlöpande dokumentera vidtagna åtgärder enligt punkt 1-4.

**9 §** En leverantör ska ha interna regler och arbetssätt som säkerställer att medarbetarna har kunskap om säker hantering av information, genom att

1. hålla relevanta interna regler och stöd för säker informationshantering kända för medarbetarna,
2. regelbundet och utifrån identifierat behov och arbetsuppgifter utveckla och upprätthålla medarbetarnas kompetens genom utbildning, informationsinsatser och övning, samt
3. följa upp och utvärdera organisationens förmåga att förmedla kunskap till medarbetarna om säker hantering av information.

**Särskilt om nätverk och informationssystem**

**10 §** En leverantör ska ha interna regler och arbetssätt som säkerställer att samtliga nätverk och informationssystem för samhällsviktiga tjänster uppfyller identifierade behov av informationssäkerhet. Drift och förvaltning över tid, arkitektur samt sammankoppling mot andra nätverk och informationssystem ska särskilt beaktas.

Arbetet ska dokumenteras.

**11 §** En leverantör ska ha interna regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser avseende informationshanteringen i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster.

Efter avslutad incidenthantering ska leverantören identifiera grundorsaker till att incidenter och avvikelser inträffat samt vidta åtgärder för att förhindra att liknande incidenter och avvikelser inträffar på nytt.

Arbetet ska dokumenteras.

**12 §** I syfte att minska effekten av en incidents negativa inverkan på den samhällsviktiga tjänsten ska en leverantör ha interna regler och arbetssätt som tydliggör hur

1. leverantören identifierar behovet av kontinuitet för den samhällsviktiga tjänsten,
2. förmågan att upprätthålla kontinuitet vid incidenter säkerställs och övas avseende information, nätverk och informationssystem, samt
3. arbetet för att minska effekterna av incidenter utvärderas och vid behov anpassas och utvecklas.

Arbetet ska dokumenteras.

---

Denna författning träder i kraft den 1 november 2018.

Myndigheten för samhällsskydd och beredskap

DAN ELIASSON

Tove Wätterstam
(Avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet)

**MSBFS**
**2018:8**

# Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster

Följande allmänna råd kompletterar Myndigheten för samhällsskydd och beredskaps föreskrifter om leverantörer av samhällsviktiga tjänsters informationssäkerhet. Termer och uttryck som används i föreskrifterna har samma betydelse här.

Allmänna råd har en annan juridisk status än föreskrifter. Allmänna råd är inte tvingande. Deras funktion är att förtydliga innebörden i lag, förordning eller myndighetsföreskrifter och att ge generella rekommendationer om deras tillämpning.

Allmänna råd är markerade med grå bakgrund.

Myndigheten för samhällsskydd och beredskap

ÅKE HOLMGREN

Tove Wätterstam
(Avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet)

### Tillämpningsområde

*2 § Utkontraktering*

I avtalet mellan leverantören och den externa aktören bör tydliggöras hur uppföljning av överenskomna säkerhetsåtgärder och det systematiska och riskbaserade informationssäkerhetsarbetet ska ske. Dessutom bör det framgå hur den externa aktören ska överlämna information till leverantören om misstänkta eller inträffade incidenter, avvikelser och sårbarheter. Krav på tillräcklig kunskap och kompetens avseende informationssäkerhet bör också framgå av avtalet.

Har avtal ingåtts med extern aktör innan denna författning har trätt i kraft bör leverantören analysera hur avtalet förhåller sig till kraven i denna författning samt vidta nödvändiga säkerhetsåtgärder.

### Systematiskt och riskbaserat informationssäkerhetsarbete

*5 § Användning av standarder*

Om en leverantör valt att använda en annan standard än de som anges i 5 § i denna författning bör leverantören analysera och dokumentera de likheter och skillnader som finns mellan respektive standarder. Analysen bör ge underlag för att säkerställa att vald standard ger tillräckligt stöd i arbetet.

Arbetet med informationssäkerhet bör integreras med leverantörens befintliga sätt att leda och styra sin organisation.

*6 § Intern ledning och styrning av informationssäkerhetsarbetet*

Då en leverantör identifierar organisationens behov av informationssäkerhet bör rättsliga krav, gällande avtal, samt interna regelverk som styr hur leverantören hanterar sin information beaktas.

En leverantör bör ha interna regler och arbetssätt som säkerställer att medarbetare med särskilt utpekade funktioner i informationssäkerhetsarbetet har tillräcklig kunskap och kompetens om säker informationshantering för att kunna utföra sina arbetsuppgifter.

En leverantör bör minst en gång per år utvärdera informationssäkerhetsarbetet, inklusive interna regler och stöd. Utvärdering bör också ske i samband med verksamhetsuppföljning, omorganisationer, förändrade rättsliga krav, förändringar rörande nätverk och informationssystem samt vid utkontraktering.

Utvärderingen bör omfatta både styrningen av informationssäkerhetsarbetet och effekten av införda säkerhetsåtgärder.

Utvärderingen bör ske genom interna kontroller, granskningar, interna och externa revisioner eller motsvarande. Interna regler och arbetssätt bör tydliggöra hur valet av metod för utvärdering ska ske.

**Närmare krav på informationssäkerhetsarbetet**

*7 § Styrande dokument*

Det bör framgå vilka interna regler och arbetssätt för informationssäkerhetsarbetet som är styrande respektive vägledande.

*8 § Systematiskt arbetssätt*

Av interna regler och arbetssätt för informationsklassning och riskbedömning bör framgå

- kriterier och nivåer som bedömningarna ska utgå från,
- när i tid och i vilka situationer informationsklassning och riskbedömning ska genomföras, samt
- vilken funktion som ansvarar för att informationsklassning och riskbedömning genomförs.

Den konsekvensbedömning som genomförs vid informationsklassning bör ha sin utgångspunkt i riskbedömningens kriterier och nivåer.

Verksamhetens behov av spårbarhet samt äkthet och ursprung (autenticitet) hos informationen bör särskilt beaktas.

Vid bedömning av risker bör även hot och sårbarheter identifieras och värderas.

Vid val av ändamålsenliga och proportionella säkerhetsåtgärder bör leverantören kombinera organisatoriska, fysiska och tekniska åtgärder.

Den åtgärdsplan som följer av genomförd riskbedömning bör omhänderta samtliga behov av att utveckla säkerheten i nätverks- och informationssystem och tydliggöra vilken funktion som ansvarar för att valda säkerhetsåtgärder införs och utvärderas.

För att underlätta informationssäkerhetsarbetet bör leverantören gruppera beslutade säkerhetsåtgärder i skyddsnivåer och koppla dem till informationsklassningens konsekvensnivåer. Förmågan att med beslutade skyddsåtgärder upprätthålla tillräckligt skydd på respektive skyddsnivå bör regelbundet utvärderas och vid behov utvecklas.

*9 § Kunskap och kompetens*

Uppföljning och utvärdering av organisationens förmåga att förmedla kunskap om säker hantering av information bör genomföras minst vartannat år.

### Särskilt om nätverk och informationssystem

*10 § Informationssäkerhet för nätverk och informationssystem*

En leverantörs arbetssätt bör säkerställa att den tekniska utvecklingen beaktas och att tekniska hot och sårbarheter löpande identifieras och omhändertas.

En leverantör bör säkerställa att det finns korrekt och tillräcklig dokumentation avseende nätverk och informationssystem.

En leverantör bör upprätta separata miljöer för tester och utveckling som är skild från produktionsmiljön.

Vid val av säkerhetsåtgärder i form av krypto- och it-säkerhetsprodukter, bör alltid behovet av att välja produkter som är certifierade genom tredjepartsgranskning mot lämplig standard analyseras.

*11 § Incidenthantering*

Interna regler och arbetssätt bör innehålla krav på loggning i syfte att identifiera och verifiera händelser i nätverk och informationssystem. I detta ingår att säkerställa enhetlig användning av korrekt och spårbar tid för att möjliggöra jämförbarhet mellan loggar från leverantörens nätverk och informationssystem.

Inträffade incidenter och avvikelser bör föranleda översyn av det systematiska och riskbaserade arbetssättet samt införda säkerhetsåtgärder.

I syfte att utveckla skyddet av information, nätverk och informationssystem bör den som utsetts att leda och samordna informationssäkerhetsarbetet hos leverantören ha åtkomst till information om inträffade incidenter och avvikelser.

*12 § Kontinuitetshantering*

Vid bedömning av behovet av kontinuitet i den samhällsviktiga tjänsten bör både kvantitet och kvalitet beaktas liksom avtalad utfästelse avseende leveransen.

Av interna regler och arbetssätt för att uppnå kontinuitet för information, nätverk och informationssystem vid incidenter och avvikelser bör framgå

- accepterad återställandetid,
- hur beslut om att tillämpa alternativa arbetssätt respektive beslut om att återgå till normalt arbetssätt fattas, samt
- behovet av uthållighet över tid.

Utvärdering av kontinuitetsarbetet bör särskilt ske efter genomförda övningar, vid organisationsförändringar inklusive utkontraktering, vid förändrade rättliga krav eller verksamhetskrav, samt om brister upptäcks i samband med att alternativa arbetssätt används.