

Livsmedelsverkets författningssamling

ISSN 1651-3533

Livsmedelsverkets föreskrifter om informationssäkerhet för samhällsviktiga tjänster inom leverans och distribution av dricksvatten;

LIVSFS 0000:0

Utkom från trycket

beslutade den .

Med stöd av 8 § förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster föreskriver Livsmedelsverket följande.

Föreskrifternas innehåll och tillämpningsområde

1 § I dessa föreskrifter finns bestämmelser om informationssäkerhet för samhällsviktiga tjänster inom leverans och distribution av dricksvatten i enlighet med 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.

2 § Föreskrifterna gäller för leverantörer som identifierats som en leverantör av samhällsviktiga tjänster inom leverans och distribution av dricksvatten i 8 kap.

1 § Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:7) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

Dessa föreskrifter gäller dock inte för verksamhet som omfattas av undantagen i 8 och 9 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Uttryck i föreskrifterna

3 § Uttryck som används i föreskrifterna har samma innebörd som i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

I dessa föreskrifter avses med

1. *leverantör*: en aktör som identifierats som en leverantör av samhällsviktiga tjänster inom leverans och distribution av dricksvatten i 8 kap. 4 § MSBFS 2018:7, och
2. *underleverantör*: en aktör som förser en leverantör med varor eller tjänster och som inte står under direkt organisatorisk kontroll under leverantören.

Förteckningar

4 § Leverantören ska föra aktuella förteckningar över

- tillgångar i form av nätverksansluten hård- och mjukvara,
- förbindelser i form av kommunikationslänkar,
- beroenden till underleverantörer, och
- vilka delar av den egna organisationen (organisatorisk enhet)

som kan påverka säkerheten i den samhällsviktiga tjänsten.

Förteckningarna ska omfatta en aktuell kartläggning av logiska samband och kommunikationer till och från systemkomponenter.

Sårbarheter

5 § För varje tillgång, förbindelse, underleverantör och organisatorisk enhet i förteckningarna enligt 4 § ska kända och potentiella tekniska, organisatoriska och administrativa sårbarheter, som kan ha en negativ effekt på den samhällsviktiga tjänsten, systematiskt kartläggas och dokumenteras.

Riskanalysmetoder

6 § Leverantören ska ha minst en i förväg beslutad riskanalysmetod som är tillämpbar på tillgångar, förbindelser, underleverantörer och organisatoriska enheter i förteckningarna enligt 4 §.

Riskanalysmetoden ska vara utformad på ett sådant sätt att den med samma ingångsvärden, kompetens hos medverkande och avgränsning genererar konsekventa och sinsemellan jämförbara resultat.

Riskanalyser

7 § Leverantören ska ha en plan för vid vilka tidpunkter och i vilka situationer leverantören ska genomföra riskanalyser.

8 § Leverantören ska, utöver den årliga riskanalysen som ska utföras enligt 12 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, genomföra riskanalyser inför planerade förändringar som kan påverka driftsäkerheten för leverans och distribution av dricksvatten.

9 § De riskanalyser som genomförs ska sammantaget omfatta de tillgångar och förbindelser som framgår av förteckningarna enligt 4 §.

För varje enskild riskanalys ska det finnas en dokumenterad beskrivning av vilka tillgångar och förbindelser som den omfattar.

10 § En riskanalys ska innehålla följande delar:

1. samtliga rimligen identifierbara omständigheter eller händelser som har betydelse för nätverk och informationssystem och som kan påverka leverans och distribution av dricksvatten negativt (risker),
2. kvalificerade bedömningar av tänkbara konsekvenser om sådana omständigheter inträffar,
3. kvalificerade bedömningar av sannolikheten för att sådana omständigheter inträffar, samt
4. kvalificerade sammanvägda bedömningar av sannolikheten för att omständigheterna inträffar och de negativa konsekvenser detta kan medföra (riskbedömning).

11 § Utöver vad leverantören identifierat enligt 10 § 1, ska en riskanalys även beakta ytterligare faktorer som kan ha inverkan på leverantörens förmåga att leverera och distribuera dricksvatten, såsom

- erfarenheter från inträffade incidenter,
- aktuell omvärldsbevakning,
- sårbarheter som kartlagts enligt 5 §,
- sammankoppling med andra verksamheters nätverk och informationssystem, och
- tidigare införda åtgärder som kan behöva uppdateras.

12 § Resultatet av riskanalysen och vilka som deltagit vid genomförandet av riskanalysen ska dokumenteras.

Riskägare

13 § För varje riskbedömning i riskanalysen ska det finnas en beslutad och dokumenterad riskägare som har rätt att fatta beslut om åtgärder.

Åtgärdsplan

14 § Leverantören ska upprätta och dokumentera en åtgärdsplan som baseras på resultatet av genomförda riskanalyser.

Åtgärdsplanen ska innehålla följande uppgifter:

- vilka risker som respektive åtgärd avser hantera och hur,
- redan införda åtgärder och hanterade risker,
- planerad sluttid för införande eller genomförande av respektive åtgärd,

- vem inom den egna organisationen som ansvarar för genomförandet av respektive åtgärd, och
- underleverantörers åtaganden för genomförandet av en eller fler åtgärder.

Säkerhetsåtgärder

15 § I 16–18 §§ uppställs krav på grundläggande säkerhetsåtgärder som leverantören måste vidta för att hantera risker i nätverk och informationssystem. Dessa säkerhetsåtgärder ska vidtas oavsett vilka ytterligare åtgärder som bedöms lämpliga utifrån leverantörens riskanalys.

16 § Leverantören ska se till att nätverks- och informationssystem som används för leverans och distribution av dricksvatten är logiskt eller fysiskt separerade från informationssystem eller nätverk som inte omfattas av motsvarande krav på informationssäkerhet.

17 § Åtkomst till nätverks- och informationssystem som har betydelse för den samhällsviktiga tjänsten ska endast medges till den eller det som behöver sådan åtkomst för att kunna utföra sina arbetsuppgifter. Tilldelad behörighet ska begränsas till det som är nödvändigt.

Leverantören ska ha fastställda regler för tilldelning, ändring och uppföljning av åtkomst och behörighet enligt första stycket.

18 § Leverantören ska se till att autentisering vid fjärråtkomst till informationssystem som har betydelse för den samhällsviktiga tjänsten baseras på flera faktorer (flerfaktorsautentisering).

-
1. Dessa föreskrifter träder i kraft den 1 augusti 2020.
 2. De åtgärder som avses i 16–18 §§ ska vara genomförda senast den 1 januari 2021.

ANNICA SOHLSTRÖM

Elin Häggqvist
(Juridiska avdelningen)