Gemensamma författningssamlingen avseende hälso- och sjukvård, socialtjänst, läkemedel, folkhälsa m.m.

ISSN 2002-1054, Artikelnummer 2024-xx-xxxx
Utgivare: Chefsjurist Pär Ödman, Socialstyrelsen

Socialstyrelsens föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn;

HSLF-FS 2024:xx

Utkom från trycket den xx xxxx 0xx

beslutade den xx xxxx 2024.

Socialstyrelsen föreskriver följande med stöd av 8 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Innan föreskrifterna meddelades fick Myndigheten för samhällsskydd och beredskap tillfälle att yttra sig.

Tillämpningsområde och definitioner

1 § I dessa föreskrifter finns kompletterande bestämmelser till 12–14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Föreskrifterna ska tillämpas av sådana leverantörer som avses i 3 § 1 lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, när de tillhandahåller samhällsviktiga tjänster inom hälso- och sjukvårdssektorn.

2 § De uttryck som används i föreskrifterna har samma betydelse som i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Ledningssystem

3 § Av Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete framgår det att varje vårdgivare ska ansvara för att det finns de processer och rutiner som behövs för att säkra verksamhetens kvalitet.

I Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster finns närmare 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.

Identifiering och förteckning

4 § Varje leverantör ska identifiera vilka av dennes nätverk och informationssystem som används för att tillhandahålla en samhällsviktig tjänst och säkerställa dess kontinuitet.

5 § Leverantören ska med utgångspunkt från identifieringen i 4 § upprätta en förteckning över nätverken och informationssystemen.

I förteckningen ska varje nätverk och informationssystem anges med en unik beteckning. Nätverkets eller informationssystemets funktionalitet ska framgå av förteckningen.

Förteckningen ska uppdateras årligen.

Riskanalys och åtgärdsplan

6 § Av 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår det att varje leverantör ska göra en riskanalys. Vidare framgår det av samma paragraf i lagen att det i analysen ska ingå en åtgärdsplan samt att analysen ska dokumenteras och uppdateras årligen.

7 § Leverantören ska välja en riskanalysmetod som utgår från en etablerad standard.

Valet av metod ska dokumenteras samt uppdateras kontinuerligt. Uppgiften ska bevaras i fem år från den tidpunkt den har tagits fram.

8 § I riskanalysen ska leverantören

1. ge en beskrivning av de risker som kan påvisas och som skulle kunna ha en negativ inverkan på säkerheten i identifierade nätverk och informationssystem,
2. redogöra för tänkbara konsekvenser av påvisade risker,
3. göra en bedömning av sannolikheten för att påvisade risker realiseras, och
4. göra en sammanvägning av vad som anges i 2 och 3.

I riskanalysen ska leverantören vidare beakta omvärldsföreteelser och incidenter som kan påverka upprätthållandet av säkerheten i de identifierade nätverken och informationssystemen.

Riskanalysen ska dokumenteras. Den ska bevaras i fem år från den tidpunkt den har tagits fram. Detta gäller även för uppdaterade versioner.

9 § I åtgärdsplanen ska leverantören göra en bedömning av om påvisade risker ska elimineras, reduceras eller accepteras. Av planen ska det framgå

1. vilka risker som en eller flera åtgärder avser att hantera,
2. vilket identifierat nätverk respektive informationssystem som berörs av en eller flera åtgärder,
3. vilken eller vilka åtgärder som leverantören har valt att vidta,
4. vilken motivering som ligger till grund för valet av åtgärden eller åtgärderna,
5. hur risknivån förväntas förändras mot bakgrund av åtgärden eller åtgärderna,
6. vem i organisationen som är ansvarig för att vidta en viss åtgärd,
7. när varje åtgärd är planerad att vidtas,
8. när varje åtgärd har vidtagits,
9. vilken eller vilka risker som tidigare har hanterats, och
10. vilken eller vilka åtgärder som tidigare har vidtagits.

Leverantören ska årligen följa upp och utvärdera vidtagna åtgärder.

Säkerhetsåtgärder

Val av åtgärder

10 § Om en leverantörs riskanalys påvisar risker som bör elimineras eller reduceras, ska leverantören vidta åtgärder för att hantera dem i enlighet med vad som anges i 11–21 §§. Om vad som sägs i de paragraferna är otillräckligt, ska leverantören vidta de ytterligare säkerhetsåtgärder som är nödvändiga.

Vid bedömningen av vilka säkerhetsåtgärder som ska vidtas ska leverantören beakta samtliga tekniska lösningar som vid var tid finns tillgängliga på marknaden.

Fysiska och logiska skydd

11 § Leverantören ska vidta säkerhetsåtgärder för att skydda de identifierade nätverken och informationssystemen mot intrång, överbelastningsattacker och andra hot.

Programvaruhantering

12 § Leverantören ska vidta säkerhetsåtgärder för att säkerställa att kända allvarliga brister eller sårbarheter i de identifierade informationssystemens programvara omhändertas.

Leverantören ska ta fram processer och rutiner för säker programvaruhantering.

Processerna och rutinerna ska dokumenteras.

Behörighets- och åtkomsthantering

13 § Leverantören ska ansvara för att varje person som behöver ha tillgång till de identifierade nätverken och informationssystemen tilldelas en individuell behörighet. Beslutet om tilldelningen av behörigheten ska föregås av en behovs- och riskanalys. En behörighet ska begränsas till vad en person behöver för att kunna fullgöra sina arbetsuppgifter.

Vad gäller systemadministration ska behörighet tilldelas restriktivt och endast till den som har till uppgift att utföra sådan administration.

Uppgifter om tilldelade behörigheter ska dokumenteras.

14 § Leverantören ska ta fram rutiner för tilldelning, ändring, borttagning och regelbunden uppföljning av samtliga behörigheter för att säkerställa att de är korrekta.

15 § Leverantören ska vidta de säkerhetsåtgärder som behövs så att obehöriga inte får tillgång till de identifierade nätverken och informationssystemen.

Tester och kontroller

16 § Leverantören ska genomföra nätverks- och systemtester samt kvalitetskontroller inför och efter tekniska eller organisatoriska förändringar som skulle kunna få negativa konsekvenser för informationssäkerheten. Leverantören ska vidare ta fram en process för hanteringen av sådana förändringar. Vid framtagandet av processen ska leverantören använda en metod som utgår från en etablerad standard.

Leverantören ska även ta fram en plan för att kunna återställa de identifierade nätverken och informationssystemen i händelse av att förändringarna ger upphov till en incident.

Planen ska dokumenteras.

Kompetens och personella resurser

17 § Leverantören ska vad gäller de identifierade nätverken och informationssystemen se till att

1. de som utför arbetsuppgifter för att upprätthålla säkerheten i dem har tillräcklig kompetens,
2. tillräckliga personella resurser finns tillgängliga för att upprätthålla säkerheten i dem, och
3. de som utför arbetsuppgifter för att upprätthålla säkerheten i dem känner till och tillämpar framtagna processer och rutiner.

Spårbarhet

18 § För att upprätthålla säkerheten i de identifierade nätverken och informationssystemen ska leverantören lagra uppgifter i filer, loggar, som visar

1. vilka ändringar som har gjorts av uppgifter som är relevanta för att upprätthålla säkerheten i nätverken och informationssystemen och när de har gjorts,
2. systemhändelser som är relevanta för att kunna utreda intrång och när de har ägt rum, och
3. om och när någon har tagit del av konfidentiella uppgifter.

Om det inte är omöjligt att identifiera en användare i 1–3, ska även användaren framgå av loggarna.

19 § Leverantören ska ta fram processer och rutiner för hur uppgifter ska lagras i loggar.

Processerna och rutinerna ska dokumenteras samt uppdateras kontinuerligt.

Leverantören ska se till att loggarna skyddas från obehörig åtkomst. De ska vidare följas upp genom systematiska och återkommande stickprovskontroller. Loggarna ska bevaras i tio år från den tidpunkt de skapades.

Konsekvensminimering

Övervakning, larm och incidenthantering

20 § Leverantören ska ta fram rutiner som möjliggör att incidenter som kan påverka upprätthållandet av säkerheten i de identifierade nätverken och informationssystemen upptäcks och hanteras skyndsamt. Leverantören ska även ta fram rutiner för intern rapportering, analys och hantering av incidenter. Vid framtagandet av rutinerna ska leverantören använda en metod som utgår från en etablerad standard.

Rutinerna ska dokumenteras samt uppdateras kontinuerligt.

Leverantören ska efter en incident vidta åtgärder för att undvika liknande händelser i framtiden.

Kontinuitetsplanering

21 § Leverantören ska ta fram planer för hur en samhällsviktig tjänsts kontinuitet ska säkerställas i samband med större och mindre incidenter. Av varje kontinuitetsplan ska det för de identifierade nätverken och informationssystemen framgå

1. vilken återställandetid som är acceptabel i dem,

2. när och hur alternativa arbetssätt ska användas för att säkerställa kontinuiteten i tjänsten,
3. hur alternativa arbetssätt för att säkerställa kontinuiteten i tjänsten ska övas, och
4. hur arbetet med att säkerställa kontinuiteten i tjänsten ska utvärderas och vid behov utvecklas.

Vid framtagandet av planerna ska leverantören använda en metod som utgår från en etablerad standard.

Kontinuitetsplanerna ska dokumenteras samt uppdateras kontinuerligt.

Denna författning träder i kraft den 1 juli 2024.

Socialstyrelsen

OLIVIA WIGZELL

Emmelie Pettersén Uggla