MSBFS
Remissutgåva

Förslag till Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster

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

Tillämpningsområde

1 § Denna författning innehåller bestämmelser om tillämpningen av kravet i 11 § lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Bestämmelserna avser det systematiska och riskbaserade informationssäkerhetsarbete som leverantörer av samhällsviktiga tjänster ska bedriva.

2 § Det systematiska och riskbaserade informationssäkerhetsarbetet som en leverantör av samhällsviktiga tjänster bedriver ska även omfatta sådan hantering av information som utkontrakteras till en extern aktör.

Begreppsförklaring

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

4 § I denna författning avses därutöver med:

informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss typ av information.
informationssäkerhet	Bevarande av konfidentitalitet, riktighet och tillgänglighet hos information.
kontinuitet i samhällsviktig tjänst	Förmåga hos leverantören att under störning och efter avbrott fortsätta tillhandahålla den

	samhällsviktiga tjänsten i en i förväg accepterad omfattning.
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	Med leverantör avses en organisation som uppfyller kraven i Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:xxx) 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 om ledningssystem för informationssäkerhet, SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 eller motsvarande.

Det systematiska och riskbaserade informationssäkerhetsarbetet ska utformas och samordnas utifrån organisationens behov och vara styrande avseende 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 den övriga organisationens ansvar för informationssäkerhetsarbetet,
2. tilldela nödvändiga resurser, mandat och befogenheter för de roller som arbetet med informationssäkerhet kräver,
3. säkerställa att informationssäkerhetsarbetet inklusive tillhörande regler och stöd regelbundet utvärderas och löpande anpassas.

Arbetet ska dokumenteras.

Närmare krav på informationssäkerhetsarbete

7 § En leverantör ska upprätta en informationssäkerhetspolicy där ledningens målsättning med och inriktning för organisationens informationssäkerhetsarbete framgår. Leverantören ska också upprätta de regler och det stöd som i övrigt krävs för organisationens informationssäkerhetsarbete.

8 § En leverantör ska ha ett dokumenterat arbetssätt som stöd för arbetet att

1. vid behov klassa information med utgångspunkt i vilka konsekvenser som kan uppkomma vid brister i konfidentialitet, riktighet och tillgänglighet,
2. årligen och vid behov 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 denna bestämmelse punkt 1-4.

9 § En leverantör ska eftersträva ett högt säkerhetsmedvetande där alla i organisationen har kunskap om och förståelse för behoven av säker hantering av information, genom att

1. relevanta regler för säker informationshantering är kända av medarbetarna,
2. regelbundet och utifrån identifierat behov genomföra utbildningar rörande informationssäkerhet som är anpassade till medarbetarnas arbetsuppgifter, samt
3. regelbundet följa upp och utvärdera organisationens förmåga att upprätthålla lämpligt skydd för sin information. Resultatet av utvärderingen ska användas som underlag för att utveckla leverantörens informationssäkerhetsarbete.

Särskilt om nätverk och informationssystem

10 § En leverantör ska ha regler och arbetssätt som säkerställer att samtliga berörda nätverk och informationssystem uppfyller organisationens behov av säker hantering av information.

Vid val av säkerhetsåtgärder i nätverk och informationssystem ska drift och förvaltning över tid, arkitektur och sammankoppling mot externa nätverk särskilt beaktas.

Arbetet ska dokumenteras.

11 § En leverantör ska ha regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser som påverkar organisationens tillhandahållande av samhällsviktiga tjänster.

Arbetssättet ska säkerställa förmåga att rapportera incidenter till extern aktör.

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

Arbetet ska dokumenteras.

12 § En leverantör ska ha regler och arbetssätt som minskar effekten av störningar i samhällsviktiga tjänster genom att tydliggöra

1. hur organisationen identifierar sitt behov av kontinuitet för information, nätverk och informationssystem,
2. när och hur alternativa arbetssätt ska användas för att upprätthålla kontinuiteten vid störningar och avbrott,
3. hur organisationen säkerställer lämpligt skydd för sin information när alternativa arbetssätt används,
4. hur alternativa arbetssätt för att upprätthålla kontinuitet övas, samt
5. hur arbetet för att upprätthålla kontinuitet utvärderas samt vid behov anpassas och utvecklas.

Arbetet ska dokumenteras.

ARBETSMATERIAL

Allmänna råd

MSBFS
Remissutgåva

Förslag till 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.

Tillämpningsområde

Innan uppdrag ges till en extern aktör att hantera organisationens information bör leverantören analysera och dokumentera de risker som detta innebär. Med extern aktör avses även inhyrda konsulter eller motsvarande.

I avtalet mellan leverantören och den externa aktören bör tydliggöras hur uppföljning av avtalade säkerhetsåtgärder och systematiskt och riskbaserat informationssäkerhetsarbete 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 de krav som ställts på informationssäkerhet och genomföra en riskbedömning. Riskbedömningen bör ligga till grund för framtida hantering av avtalen.

Systematiskt och riskbaserat informationssäkerhetsarbete

Om en leverantör valt att använda en annan standard än den 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.

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

En leverantör bör ha regler och arbetssätt som säkerställer att personal med särskilt utpekade roller i informationssäkerhetsarbetet har tillräckligt med mandat, kunskap och kompetens för att kunna utföra sina arbetsuppgifter.

En leverantör bör utvärdera informationssäkerhetsarbetet flera gånger per år och vid behov, till exempel i samband med verksamhetsuppföljning, omorganisationer, förändrade rättsliga krav, förändringar av nätverk och informationssystem samt vid utkontraktering.

Leverantören bör välja det sätt att utvärdera och följa upp informationssäkerheten som bäst uppfyller behovet, till exempel genom kontroller, granskningar, interna eller externa revisioner.

Närmare krav på informationssäkerhetsarbetet

Regler för informationssäkerhetsarbetet bör utformas i enlighet med leverantörens hierarki för regeldokument.

Av regler och arbetssätt för informationsklassning och riskbedömning bör följande framgå.

- Kriterier och nivåer som bedömningarna ska utgå från.
- När i tid och i vilka situationer informationsklassning och riskbedömning ska genomföras.
- Vilken roll som ansvarar för att informationsklassning och riskbedömning genomförs.

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

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

Den åtgärdsplan som följer av genomförd riskbedömning bör omhänderta samtliga behov av att utveckla säkerheten i nätverks- och informationssystem.

Av regler och arbetssätt bör framgå vilken roll 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.

En leverantör bör på ett spårbart sätt säkerställa att samtliga medarbetare har informerats om regler inklusive leverantörens informationssäkerhetspolicy, samt det stöd som i övrigt finns för att hantera information på ett säkert sätt.

En leverantör bör också se till att samtliga medarbetare får relevant utbildning för att på ett säkert sätt kunna utföra den informationshantering som följer av medarbetarens arbetsuppgifter.

Utbildning i informationssäkerhet bör återkomma minst vartannat år.

Särskilt om 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 produkter, särskilt krypto- och it-säkerhetsprodukter, bör i första hand produkter som är certifierade genom tredjepartsgranskning mot lämplig standard och bedömt behov av skydd väljas.

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.

Krav på rapportering av incidenter enligt 18 § lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster bör särskilt beaktas.

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

En leverantör bör säkerställa att det finns rutiner för att polisanmäla incidenter som kan antas ha sin grund i en brottslig gärning.

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.

Leverantören bör säkerställa att regler och arbetssätt för att upprätthålla kontinuitet för information, nätverk och informationssystem tydliggör

– accepterad återställandetid, samt

– hur beslut om att tillämpa alternativa arbetssätt respektive beslut om att återgå till normalt arbetssätt bör fattas.

Vid utformning av alternativa arbetssätt bör organisationens behov av uthållighet särskilt beaktas.

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