Post- och telestyrelsens författningssamling

ISSN 1400-187X

Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster;

PTSFS 2022:11

Utkom från trycket
den 30 juni 2022

beslutade den 21 juni 2022.

Post- och telestyrelsen föreskriver[1] följande med stöd av 1 kap. 8 § och 8 kap. 4–6 §§ förordningen (2022:511) om elektronisk kommunikation och beslutar följande allmänna råd.

1 kap. Tillämpningsområde

1 § Dessa föreskrifter innehåller bestämmelser om

– tekniska och organisatoriska åtgärder som enligt 8 kap. 1 § lagen (2022:482) om elektronisk kommunikation ska vidtas för att hantera risker som hotar säkerheten i nät och tjänster,

– rapportering enligt 8 kap. 3 § lagen om elektronisk kommunikation av säkerhetsincidenter som har haft en betydande påverkan på kommunikationsnät och kommunikationstjänster,

– skyldighet enligt 8 kap. 4 § lagen om elektronisk kommunikation för tillhandahållare att informera användare vid ett konkret och betydande hot om en säkerhetsincident,

– särskilda tekniska och organisatoriska åtgärder som enligt 8 kap. 5 § lagen om elektronisk kommunikation ska vidtas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,

– tekniska och organisatoriska åtgärder som enligt 8 kap. 6 § lagen om elektronisk kommunikation ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av kommunikationstjänsten skyddas,

– innehållet i förteckningen över integritetsincidenter enligt 8 kap. 9 § lagen om elektronisk kommunikation, och

– fredstida planering enligt 1 kap. 11 § lagen om elektronisk kommunikation för totalförsvarets behov av elektroniska kommunikationer.

[1] Se Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

2 kap. Ord och uttryck

1 § Ord och uttryck i dessa föreskrifter har samma betydelse som i lagen (2022:482) om elektronisk kommunikation och förordningen (2022:511) om elektronisk kommunikation.

2 § I dessa föreskrifter avses med

aktiv anslutning: anslutning till kommunikationsnät eller kommunikationstjänst, som inte är en nummeroberoende interpersonell kommunikationstjänst, och som möjliggör omedelbar användning av kommunikationstjänster,

behandlade uppgifter: uppgifter som behandlas i samband med tillhandahållande av kommunikationsnät eller kommunikationstjänster,

fel i extern elförsörjning: störning eller avbrott i extern elförsörjning,

förbindelse: del av kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett kommunikationsnät,

informationsbehandlingstillgångar: system, databaser och fysiska resurser som används för informationsbehandling,

kapacitetsbortfall: reducerad förmåga att tillhandahålla visst kommunikationsnät eller viss kommunikationstjänst, angiven som

– andel i förhållande till normal nivå vid tillhandahållande av kommunikationsnätet eller kommunikationstjänsten eller som

– andel aktiva anslutningar eller användare i förhållande till det totala antalet aktiva anslutningar eller användare för kommunikationsnätet eller kommunikationstjänsten som till följd av avbrottet eller störningen inte kan nyttja tjänsten,

kommunikationsnät: sådant allmänt elektroniskt kommunikationsnät som avses i 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation,

kommunikationstjänst: sådan elektronisk kommunikationstjänst som avses i 1 kap. 7 § lagen om elektronisk kommunikation,

kritisk komponent: del av en tillgång som är nödvändig för att sända, motta, bearbeta eller lagra information,

redundans: två eller flera, identiska eller olika, sätt att oberoende av varandra fylla samma funktion,

reservkraftsystem: system som oberoende av extern elförsörjning genererar elektricitet vid fel i den externa elförsörjningen,

session: pågående informationsöverföring mellan minst två parter genom en kommunikationstjänst,

tillgång: funktion som utgörs av en avgränsad del av ett kommunikationsnät eller en kommunikationstjänst och som är nödvändig för att tillhandahålla ett sådant nät eller en sådan tjänst, samt som används för att sända, motta, bearbeta eller lagra information,

tillhandahållare: den som tillhandahåller kommunikationsnät eller kommunikationstjänster,

uppdragstagare: den som anlitats av tillhandahållaren för att utföra installation, underhåll, felavhjälpning, drift eller liknande hantering av tillhandahållarens tillgångar, informationsbehandlingstillgångar och förbindelser,

vardag: dag som inte är lördag, söndag, midsommarafton, julafton, nyårsafton eller annan allmän helgdag.

3 kap. Övergripande säkerhetsarbete

1 § Tillhandahållarens säkerhetsarbete ska bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala förhållanden som extraordinära händelser.

Allmänt råd till 1 §
Till stöd för det långsiktiga, kontinuerliga och systematiska säkerhetsarbetet bör tillhandahållaren utgå från etablerad standard på området.

2 § Tillhandahållaren ska i säkerhetsarbetet ha en tydlig rollfördelning med särskilt utpekade ansvariga för arbetet. Rollfördelningen ska dokumenteras.

3 § Tillhandahållaren ska upprätta, dokumentera och vid behov revidera de processer, rutiner och planer som anges i dessa föreskrifter. Tillhandahållaren ska dokumentera de tester som utförs i enlighet med dessa föreskrifter.

4 § Tillhandahållaren ska säkerställa att anställda och uppdragstagare har kunskap om och tillämpar de processer, rutiner och planer som de är berörda av.

5 § Tillhandahållaren ska dokumentera de åtgärder som vidtas enligt 6 kap. 2–4 §§ och 7–12 kap. samt följa upp dessa åtgärder årligen och vid behov.

Allmänt råd till 5 §
Vid uppföljning av vidtagna åtgärder bör tillhandahållaren använda sig av erfarenheter och resultat från till exempel genomförda tester. Penetrationstester bör användas som en del av säkerhetsarbetet för att följa upp de åtgärder som har vidtagits.

4 kap. Identifiering och dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare

1 § Tillhandahållaren ska identifiera och dokumentera samtliga sina tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare.

Tillhandahållaren ska för respektive tillgång, informationsbehandlingstillgång och förbindelse åtminstone dokumentera

1. en unik beteckning,
2. dess funktion,
3. geografisk placering, om sådan finns,
4. en hänvisning till aktuell riskanalys enligt 5 kap., och
5. tillverkare.

För tillgångar ska även klass enligt 11 kap. dokumenteras.

Tillhandahållaren ska för respektive uppdragstagare åtminstone dokumentera

1. uppdragstagarens namn, organisationsnummer och kontaktuppgifter, och
2. en beskrivning av uppdraget.

Dokumentationen ska hållas uppdaterad och varje version ska bevaras i fem år från det att den upprättats eller uppdaterats.

5 kap. Riskanalys

1 § Tillhandahållaren ska genomföra riskanalyser.

I en riskanalys ska tillhandahållaren analysera risken för att tillgångar, informationsbehandlingstillgångar eller förbindelser orsakar eller drabbas av säkerhets- eller integritetsincidenter. Riskanalyser ska göras för varje tillgång, informationsbehandlingstillgång och förbindelse.

Allmänt råd till 1 §

För likvärdiga tillgångar, informationsbehandlingstillgångar och förbindelser kan en gemensam riskanalys göras.

2 § Riskanalyser ska genomföras minst en gång per år, samt

1. i samband med att sådana säkerhetsincidenter som ska rapporteras enligt 17 kap. har inträffat,
2. inför anskaffning av tillgångar, informationsbehandlingstillgångar, förbindelser och anlitande av uppdragstagare,
3. efter att tidigare okända hot som är relevanta för riskanalysen identifierats, och
4. inför planerade förändringar.

Information om sådana hot som avses i första stycket kan förmedlas av Post- och telestyrelsen.

3 § Riskanalyserna ska innefatta åtminstone

1. identifiering av relevanta hot mot den aktuella tillgången, informationsbehandlingstillgången eller förbindelsen som kan leda till att en säkerhets- eller integritetsincident inträffar,
2. en bedömning av vilka konsekvenser som kan uppstå i händelse av att identifierade hot realiseras,
3. en bedömning av sannolikheten för att identifierade hot realiseras, och
4. en sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras (riskbedömning).

4 § I riskanalyser inför planerade förändringar ska tillhandahållaren analysera risken för att förändringen orsakar en säkerhetsincident.

Riskanalyserna ska innefatta åtminstone

1. identifiering av relevanta hot mot säkerheten i tillgångar och förbindelser med anledning av den planerade förändringen,
2. en bedömning av vilka konsekvenser som kan uppstå i händelse av att identifierade hot realiseras,
3. en bedömning av sannolikheten för att identifierade hot realiseras, och
4. en sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras (riskbedömning).

Allmänt råd till 3 och 4 §§

Vid genomförandet av riskanalyser bör tillhandahållaren åtminstone analysera organisatoriska, logiska och fysiska hot.

En analys av organisatoriska hot bör åtminstone omfatta kritiska personberoenden, otillräcklig kompetensförsörjning, bristfällig incidenthantering, bristfällig behörighets- och åtkomsthantering samt bristfälliga processer för säkerhetsarbetet i övrigt.

En analys av logiska hot bör åtminstone omfatta kända sårbarheter i mjukvara, logiska överbelastningsattacker, logiska intrång, konfigurationsfel, fel och brister i hårdvara eller mjukvara (såväl egenutvecklad som utvecklad av annan) samt bristfällig segmentering av nätverk.

En analys av fysiska hot bör åtminstone omfatta hot relaterade till väder, klimatförändringar och den omgivande miljön, till exempel nederbörd, brand, vind, blixtnedslag, fukt, skadliga temperaturer, översvämningar, vattenläckor, samt ras, skred och erosion. Analysen av fysiska hot bör även omfatta intrång, sabotage och annan yttre påverkan, till exempel anlagda bränder, stöld, kabelbrott och strömavbrott. Den bör även omfatta brist på utrustning och reservdelar till följd av bristande förmåga hos underleverantörer att säkra leveranser och beroenden av en enskild leverantör.

Riskanalysen bör innehålla en beskrivning av hur tillgångarna, informationsbehandlingstillgångarna eller förbindelserna kan påverkas i samband med att identifierade hot realiseras och vilken påverkan detta kan få på kommunikationsnät och kommunikationstjänster.

5 § Vid genomförande av riskanalyser ska tillhandahållaren beakta erfarenheter från tidigare inträffade säkerhets- och integritetsincidenter, allmänt uppmärksammade säkerhets- och integritetsincidenter samt aktuella och relevanta omvärldsföreteelser.

Vid genomförande av riskanalyser ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

Tillhandahållaren ska ha en plan för vid vilka tidpunkter och i vilka situationer riskanalyser ska genomföras.

Tillhandahållaren ska dokumentera genomförda riskanalyser.

6 kap. Riskhantering och åtgärder efter riskbedömning

Riskhantering

1 § Tillhandahållaren ska utifrån riskbedömningen besluta hur respektive risk ska hanteras genom att avgöra om riskerna ska undvikas, reduceras eller accepteras. Sådana beslut ska dokumenteras. Beslut om att acceptera en risk ska motiveras.

Allmänt råd till 1 §
Tillhandahållaren bör eftersträva att reducera risker framför att acceptera dem. Tillhandahållaren bör endast acceptera risker om säkerheten i nät och tjänster i stort kan upprätthållas trots att hotet förverkligas eller incidenten inträffar.

Åtgärder efter riskbedömning

2 § Tillhandahållaren ska vidta tekniska och organisatoriska åtgärder för att hantera de risker som ska undvikas eller reduceras. Åtgärderna ska vidtas på en nivå som är anpassad till den risk som föreligger, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna.

Första stycket andra meningen gäller inte för sådana uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation. Tillhandahållaren ska för sådana uppgifter vidta åtgärder i enlighet med 9 kap. 4 § förordningen (2022:511) om elektronisk kommunikation.

Allmänt råd till 2 §
Tillhandahållarens åtgärder bör följa etablerade standarder, normer, säkerhetsvägledningar och praxis.

3 § Tillhandahållarens bedömning vid val av åtgärder ska dokumenteras samt följas upp årligen och vid behov.

Särskilda åtgärder vid planerade förändringar

4 § När tillhandahållarens riskanalys enligt 5 kap. visar att det finns risker för att planerade förändringar kan orsaka rapporteringspliktiga säkerhetsincidenter enligt 17 kap. ska tillhandahållaren utöver vad som följer av 2 § åtminstone

1. utföra tester inför förändringen och efter förändringen verifiera att den inte påverkat säkerheten negativt,
2. säkerhetskonfigurera (härda) berörda tillgångar, samt
3. ta fram planer för att återställa kommunikationsnätet och kommunikationstjänsten i händelse av att en säkerhetsincident inträffar.

Tester, härdning, och planer för återställande ska vara anpassade till den planerade förändringens art och omfattning.

Tillhandahållaren ska tillämpa en process vid genomförande av planerade förändringar (förändringshantering) som utgår från etablerad standard på området.

7 kap. Åtkomst och behörighet

1 § Tillhandahållaren ska medge åtkomst till tillgångar och behandlade uppgifter endast till den som är behörig. Tillhandahållaren ska tilldela sådan behörighet endast till de anställda eller uppdragstagare som behöver det för att kunna utföra sina arbetsuppgifter.

Tillhandahållaren ska tillämpa en process för tilldelning, ändring och uppföljning av tilldelade behörigheter enligt första stycket. Tilldelade behörigheter ska dokumenteras samt följas upp årligen och vid behov.

Tillhandahållaren ska ha system för hantering och kontroll av identiteter och behörigheter.

Allmänt råd till 1 §
Tillhandahållaren bör se till att den som kommer i kontakt med behandlade uppgifter regelbundet får utbildning och information om när och på vilket sätt behandlade uppgifter får hanteras. Den som kommer i kontakt med behandlade uppgifter bör även få utbildning i att upptäcka integritetsincidenter och att analysera tänkbara konsekvenser av en inträffad integritetsincident för abonnenter och användare.

Tilldelade behörigheter bör vara begränsade i tid och omfattning, särskilt för tillfälliga uppdragstagare. Tilldelade behörigheter bör tas bort efter utfört uppdrag.

2 § Tillhandahållaren ska säkerställa att åtkomst endast ges till den som har upplysts om tystnadsplikten i de fall 9 kap. 31 och 32 §§ lagen (2022:482) om elektronisk kommunikation är tillämpliga.

8 kap. Skyddsåtgärder mot oavsiktlig eller otillåten utplåning eller förlust

1 § Tillhandahållaren ska vidta åtgärder för att säkerställa att behandlade uppgifter som varaktigt lagras skyddas mot oavsiktlig eller otillåten utplåning eller förlust.

Allmänt råd till 1 §
Säkerställande av skydd mot oavsiktlig eller otillåten utplåning eller förlust bör ske genom säkerhetskopiering. Återläsning av säkerhetskopior bör verifieras åtminstone årligen.

2 § Uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation ska i stället för vad som framgår av 1 § skyddas mot oavsiktlig eller otillåten utplåning samt oavsiktlig förlust eller ändring genom lagring på minst två fysiskt åtskilda platser.

Första stycket gäller även loggar enligt 9 kap. 1 § avseende åtkomst till uppgifter som ska lagras för brottsbekämpande ändamål.

Säkerhetskopior eller motsvarande ska omfattas av samma skydd och utplånas samtidigt som de uppgifter som lagras för brottsbekämpande ändamål.

Allmänt råd till 2 §
Skydd för uppgifter som lagras för brottsbekämpande ändamål kan uppnås genom redundant lagring, säkerhetskopiering eller liknande.

9 kap. Loggning

1 § Tillhandahållaren ska logga

1. all läsning, kopiering, ändring och utplåning av behandlade uppgifter, och
2. åtkomst till de system som används för behandling av sådana uppgifter.

Loggning ska ske på ett sådant sätt att det går att se vem som har vidtagit vilken åtgärd med vilka uppgifter och vid vilken tidpunkt. Vid misstanke om att en integritetsincident har inträffat ska relevanta loggar alltid kontrolleras.

Tillhandahållaren ska ha rutiner för kontroll av loggar. Kontroller av loggar ska ske systematiskt och återkommande. Genomförda kontroller av loggar ska dokumenteras.

2 § Tillhandahållaren ska logga systemhändelser nödvändiga för att kunna utreda säkerhetsincidenter.

Allmänt råd till 1 och 2 §§
Tillhandahållaren bör tillämpa automatisk övervakning av loggar, i syfte att snabbt upptäcka onormala användarmönster, händelser eller serier av händelser. Detta gäller dock inte för loggar avseende åtkomst till uppgifter som ska lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation.

3 § Den som är skyldig att lagra uppgifter för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation ska säkerställa att den som har haft tillgång till sådana uppgifter inte ges tillgång till loggar avseende åtkomst till uppgifterna.

4 § Innan uppgifter som lagras för brottsbekämpande ändamål utplånas i enlighet med 9 kap. 22 § lagen (2022:482) om elektronisk kommunikation ska tillhandahållaren utföra en systematisk kontroll av loggar avseende åtkomst till uppgifterna. I samband med att uppgifterna utplånas ska även loggar utplånas.

10 kap. Kryptering

1 § Behandlade uppgifter som överförs via internet ska skyddas genom kryptering.

Uppgifterna behöver dock inte skyddas genom kryptering om det med hänsyn till uppgifternas art och sammanhang är osannolikt att överföring utan kryptering kan leda till en säkerhets- eller integritetsincident.

Allmänt råd till 1 §
Koder, lösenord och sammanställningar av uppgifter som rör en användare eller abonnent bör krypteras vid överföring via internet.

2 § Anslutningar för konfigurering och styrning av tillgångar via internet eller kommunikationsnät som även andra än tillhandahållaren har rådighet över ska skyddas genom kryptering.

3 § Loggar avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation ska skyddas genom kryptering under lagring och överföring.

4 § Kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras på ett säkert sätt.

5 § Tillhandahållaren ska ha rutiner för kryptering och hantering av krypteringsnycklar.

11 kap. Redundans och reservkraftsystem

Klassificering av tillgångar

1 § Tillgångar vars funktioner är nödvändiga för att tillhandahålla ett kommunikationsnät eller en kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst indelas i fem klasser. Indelningen sker utifrån det antal aktiva anslutningar som kan drabbas av en säkerhetsincident som innebär störning eller avbrott till följd av att tillgången upphör att fungera normalt.

Klass	Antal aktiva anslutningar
A	≥ 200 000
B	≥ 30 000
C	≥ 8 000
D	≥ 2 000
E	> 0

Allmänt råd till 1 §
I mobila accessnät bör antalet aktiva anslutningar beräknas utifrån det antal aktiva anslutningar som tillhandahållaren har dimensionerat tillgången för. Beräkningen bör även omfatta förutsägbara belastningstoppar.

2 § Tillgångar vars funktioner är nödvändiga för att tillhandahålla en nummeroberoende interpersonell kommunikationstjänst och som en tillhandahållare av sådan tjänst utövar direkt kontroll över indelas i två klasser. Indelningen sker utifrån uppskattat antal användare i Sverige som kan drabbas av en säkerhetsincident som innebär störning eller avbrott till följd av att tillgången upphör att fungera normalt.

Klass	Antal drabbade användare
A	≥ 200 000
B	≥ 30 000

Åtgärder efter klassificering av tillgångar

Redundans av tillgångar i klasserna A och B

3 § Tillhandahållaren ska med redundanta tillgångar säkerställa att tillgångar i klasserna A och B som upphör att fungera inte orsakar störning eller avbrott i en kommunikationstjänst. Störningar eller avbrott som består i att sessioner avbryts är dock tillåtna, om användare omedelbart kan upprätta nya sessioner.

Kravet i första stycket gäller endast om det är tekniskt tillämpbart.

Redundanta tillgångar i klass A ska vara placerade i geografiskt lämpligt separerade områden.

Redundans av tillgångar i klass C

4 § Tillhandahållaren ska med redundanta tillgångar eller redundanta kritiska komponenter säkerställa att tillgångar i klass C som upphör att fungera inte orsakar störning eller avbrott i en kommunikationstjänst. Störningar eller avbrott som består i att sessioner avbryts är dock tillåtna, om användare omedelbart kan upprätta nya sessioner.

Säkerställande av tillgångar i klass D

5 § Tillhandahållaren ska säkerställa att kritiska komponenter i en tillgång i klass D som upphör att fungera, inte orsakar störning eller avbrott i en kommunikationstjänst som överstiger 12 timmar om störningen eller avbrottet inträffar en vardag och 18 timmar om störningen eller avbrottet inträffar under övrig tid.

Redundans av förbindelser mellan tillgångar i klasserna A, B och C

6 § Tillhandahållaren ska med redundanta förbindelser mellan samtliga tillgångar inom och mellan klasserna A, B och C säkerställa att förbindelser som upphör att fungera inte orsakar störning eller avbrott i en kommunikationstjänst. Störningar eller avbrott som består i att sessioner avbryts är dock tillåtna, om användare omedelbart kan upprätta nya sessioner.

Redundanta förbindelser mellan samtliga tillgångar inom och mellan klasserna A och B ska vara geografiskt lämpligt separerade. Detta gäller inte förbindelser mellan tillgångar inom samma anläggning.

Säkerställande av förbindelser mellan en tillgång i klass D och tillgångar i klasserna A, B och C

7 § Tillhandahållaren ska säkerställa att förbindelser mellan en tillgång i klass D och en tillgång i klasserna A, B eller C som upphör att fungera, inte orsakar störning eller avbrott i en kommunikationstjänst som överstiger 12 timmar om störningen eller avbrottet inträffar en vardag och 18 timmar om störningen eller avbrottet inträffar under övrig tid.

Reservkraftsystem avseende tillgångar i klasserna A, B, C och D

8 § Tillhandahållaren ska med reservkraftsystem säkerställa att fel i extern elförsörjning inte orsakar störning eller avbrott i de kommunikationsnät och kommunikationstjänster som tillhandahålls, under åtminstone

1. 24 timmar för tillgångar i klasserna A och B,
2. 8 timmar för tillgångar i klass C i tätort med fler än 8 000 invånare,
3. 12 timmar för tillgångar i klass C på övriga platser,
4. 2 timmar för tillgångar i klass D i tätort med fler än 8 000 invånare, samt
5. 4 timmar för tillgångar i klass D på övriga platser.

Tiden beräknas från det att felet i den externa elförsörjningen inträffade.

Om det inträffar ett fel i extern elförsörjning mindre än fyra timmar efter ett tidigare, avseende samma tillgång, anses det utgöra samma fel.

9 § Tillhandahållaren ska utföra funktionstest av reservkraftsystem varje kvartal för tillgångar i klasserna A, B och C, samt varje år för tillgångar i klass D.

Tillhandahållaren ska årligen utföra test av reservkraftsystem genom att bryta den externa elförsörjningen eller motsvarande till tillgångar i klasserna A, B och C.

Tillhandahållaren ska tillämpa processer för planering, inrättande, tester, underhåll och utbyte av reservkraftsystem.

Reservkraftsystem avseende mobila kommunikationsnät och kommunikationstjänster

10 § Tillhandahållare av mobila kommunikationsnät och mobila kommunikationstjänster ska med reservkraftsystem, utöver vad som följer av 8 §, säkerställa att fel i extern elförsörjning inte orsakar störning eller avbrott i kommunikationsnät och kommunikationstjänster som tillhandahålls eller minskar kommunikationstjänsters täckningsområde, under åtminstone en timme i tätort med fler än 8 000 invånare och fyra timmar på övriga platser, från det att felet i extern elförsörjning inträffade. Fel i extern elförsörjning som inträffar med mindre än fyra timmars mellanrum avseende samma fysiska tillgång ska anses utgöra ett fel.

Tillhandahållaren får under felets varaktighet, om det är nödvändigt för att upprätthålla kommunikationstjänster under den tid som anges i första stycket och under förutsättning att täckningsområdet bibehålls, minska tillgångarnas elförbrukning genom att begränsa antalet frekvensband som används för kommunikationstjänsterna.

Tillhandahållaren ska tillämpa processer för planering, inrättande, underhåll och utbyte av reservkraftsystem.

Ansökan om undantag från 3–10 §§

11 § Post- och telestyrelsen kan, efter skriftlig ansökan från en tillhandahållare, medge undantag från krav på åtgärd enligt 3–10 §§ om i det enskilda fallet dess tillämpning skulle få konsekvenser som är

1. oproportionerliga i förhållande till kostnader förenade med åtgärden,
2. olämpliga med hänsyn till tillgänglig teknik,
3. olämpliga med hänsyn till annan reglering, eller
4. oproportionerliga med hänsyn till att berörda tillgångar eller förbindelser omfattas av beslut om avveckling.

12 § I de fall undantag medges ska tillhandahållaren vidta lämpliga alternativa åtgärder för att begränsa negativa effekter av att den föreskrivna åtgärden inte vidtas.

13 § Tillhandahållaren ska i ansökan redogöra för

1. vilka åtgärdskrav ansökan avser,
2. varför åtgärden är oproportionerlig eller olämplig, och
3. vilka alternativa och begränsande åtgärder enligt 12 § som tillhandahållaren avser att vidta.

Ansökan ska även innehålla en bedömning av hur säkerheten i nät och tjänster påverkas av att föreskrivna åtgärder inte vidtas.

12 kap. Övervakning och beredskap

1 § Tillhandahållaren ska kontinuerligt övervaka kommunikationstjänster och aktiva delar i kommunikationsnät för att kunna förebygga, upptäcka och åtgärda säkerhetsincidenter.

Tillhandahållaren ska ha system som skapar larm vid säkerhetsincidenter som innebär störningar eller avbrott.

Tillhandahållaren ska dygnet runt kunna initiera relevanta åtgärder för att hantera säkerhetsincidenter.

13 kap. Intern incidenthantering

1 § Tillhandahållaren ska säkerställa att

1. inträffade säkerhets- eller integritetsincidenter rapporteras internt,
2. åtgärder vidtas skyndsamt för att hantera en uppkommen säkerhets- eller integritetsincident,
3. åtgärder vidtas för att undvika liknande säkerhets- eller integritetsincidenter, och
4. erfarenheter från inträffade säkerhets- eller integritetsincidenter beaktas vid genomförande av riskanalyser enligt 5 kap.

Vid åtgärder enligt första stycket ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

Tillhandahållare av kommunikationstjänster ska också ha rutiner för identifiering av integritetsincidenter.

2 § Vid integritetsincidenter ska den som tillhandahåller en kommunikationstjänst löpande föra en förteckning i enlighet med 8 kap. 9 § lagen (2022:482) om elektronisk kommunikation. Förteckningen ska innehålla

1. datum då integritetsincidenten inträffade,
2. en beskrivning av integritetsincidenten,
3. uppskattat antal berörda abonnenter eller användare,
4. bedömda konsekvenser av integritetsincidenten,
5. orsak till att integritetsincidenten inträffade,
6. de åtgärder som vidtagits, och
7. referensnummer.

14 kap. Kontinuitetsplanering

1 § Tillhandahållaren ska identifiera de verksamhetsdelar och resurser som är nödvändiga för att kunna begränsa konsekvenserna av omfattande säkerhetsincidenter i form av störningar eller avbrott. Tillhandahållaren ska analysera vilka konsekvenser som kan uppstå när dessa verksamhetsdelar och resurser helt eller delvis blir otillgängliga. Analysen ska omfatta en bedömning av när kontinuitetsplaner enligt 2 § ska tillämpas.

Konsekvensanalysen enligt första stycket ska dokumenteras och revideras vid behov.

Allmänt råd till 1 §
En sådan verksamhetsdel och resurs som avses i 1 § kan till exempel vara en central databas över användare som, om den slutar att fungera, omöjliggör användandet av tjänsten. En sådan verksamhetsdel kan även utgöras av personella resurser som på grund av befattning, roll, funktion eller kunskap inom ett visst område är nödvändiga för att verksamheten ska fungera. Även en underleverantör av för tillhandahållaren helt nödvändig utrustning kan utgöra en sådan verksamhetsdel.

2 § Tillhandahållaren ska upprätta kontinuitetsplaner utifrån konsekvensanalysen i 1 §. Kontinuitetsplanerna ska åtminstone innehålla uppgifter om

1. de åtgärder som ska vidtas för att begränsa de konsekvenser som kan uppstå enligt konsekvensanalysen och för att återställa påverkade verksamhetsdelar eller resurser till normal funktionsförmåga,
2. när och på vilket sätt kontinuitetsplanerna ska övas, samt
3. när och på vilket sätt kontinuitetsplanerna ska revideras.

Tillhandahållaren ska utgå från etablerad standard på området vid framtagande av kontinuitetsplanerna.

Tillhandahållaren ska öva planerna minst vartannat år.

3 § Kontinuitetsplanerna ska tillämpas i enlighet med bedömningen i konsekvensanalysen.

15 kap. Fredstida planering för totalförsvarets behov av elektroniska kommunikationer

1 § Den som tillhandahåller ett kommunikationsnät eller en kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst ska utifrån konsekvensanalysen enligt 14 kap. 1 § även ta fram kontinuitetsplaner för höjd beredskap och krig. Sådana kontinuitetsplaner ska uppfylla kraven som framgår av 14 kap. 2 § första och andra styckena.

2 § Post- och telestyrelsen kan komma att informera tillhandahållare om

1. vilka verksamhetsdelar och resurser som är kritiska för totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och i krig, och
2. vad kontinuitetsplanerna ska innehålla för att tillgodose totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och i krig.

När Post- och telestyrelsen förmedlar information enligt första stycket ska tillhandahållaren revidera sina kontinuitetsplaner i enlighet med informationen.

3 § Tillhandahållaren ska ta fram planer för att vid höjd beredskap och i krig kunna ställa personal till förfogande för samverkan med Post- och telestyrelsen i den omfattning som krävs. Tillhandahållaren ska planera för att upprätthålla samverkansfunktionen dygnet runt i 90 dagar.

Allmänt råd till 3 §
Tillhandahållaren bör i sina planer ha utpekade personella resurser tillgängliga för samverkan med Post- och telestyrelsen.

Tillhandahållarens planer bör också omfatta de tekniska lösningar som krävs för kommunikation och samverkan med Post- och telestyrelsen vid höjd beredskap och i krig.

16 kap. Information till användare om skydds- eller motåtgärder vid hot om säkerhetsincidenter

1 § När en tillhandahållare upptäcker ett konkret och betydande hot om att en säkerhetsincident ska inträffa ska tillhandahållaren så snart som möjligt informera användare som kan komma att påverkas av hotet om de skydds- eller motåtgärder som tillhandahållaren rekommenderar.

Allmänt råd till 1 §
Tillhandahållaren bör försäkra sig om att informationen når ut till berörda användare. Informationen bör lämnas på ett säkert sätt så att inte informationen i sig ger upphov till nya säkerhetsincidenter. Informationen bör, om det är möjligt och lämpligt, beskriva den risk som hotet innebär och vad konsekvenserna kan bli om användarna inte vidtar rekommenderade åtgärder.

17 kap. Rapportering av säkerhets- och integritetsincidenter till Post- och telestyrelsen

Säkerhetsincidenter

1 § Tillhandahållaren ska till Post- och telestyrelsen rapportera sådana säkerhetsincidenter som anges i 5 och 6 §§.

Rapportering

2 § Vid incidentrapportering enligt 8 kap. 3 § lagen (2022:482) om elektronisk kommunikation ska tillhandahållaren lämna en inledande och en kompletterande rapport till Post- och telestyrelsen.

Allmänt råd till 2 §
Rapporterna bör lämnas i elektronisk form.

Inledande rapport

3 § Den inledande rapporten ska vara Post- och telestyrelsen till handa inom 72 timmar från det att säkerhetsincidenten upptäcktes och innehålla uppgifter om

1. när säkerhetsincidenten inträffade,
2. hur länge säkerhetsincidenten har pågått,
3. antal aktiva anslutningar eller användare som har drabbats av säkerhetsincidenten,
4. berört geografiskt område, i de fall det är relevant,
5. vilka säkerhetsaspekter (tillgänglighet, autenticitet, riktighet eller konfidentialitet) som har berörts av säkerhetsincidenten,
6. vilka kommunikationsnät, kommunikationstjänster, lagrade, överförda eller behandlade uppgifter eller närliggande tjänster som har berörts av säkerhetsincidenten,
7. säkerhetsincidentens påverkan på kommunikationsnätet eller kommunikationstjänsten eller påverkan på funktioner i samhället,
8. tillhandahållarens preliminära bedömning av orsaken till säkerhetsincidenten,
9. hur säkerhetsincidenten har påverkat berörda aktiva anslutningar eller användare i Sverige,
10. huruvida säkerhetsincidenten har medfört begränsningar i möjligheten till nödkommunikation via det kommunikationsnät eller den kommunikationstjänst som berörts av säkerhetsincidenten, och
11. tillhandahållarens kontaktuppgifter och referensnummer för ärendet.

Allmänt råd till 3 §
Tillhandahållaren bör göra en uppskattning av tidpunkten för när säkerhetsincidenten har inträffat i de fall en exakt tidpunkt inte kan fastställas med stöd av system för övervakning eller loggning. Uppskattningen bör göras med utgångspunkt från kända fakta om incidenten.

Redogörelsen enligt 3 § 6 bör innehålla såväl uppgifter om de berörda nätteknologierna som uppgift om berörda slutanvändartjänster, till exempel rösttelefoni, meddelandetjänst eller internetanslutning.

Kompletterande rapport

4 § Den kompletterande rapporten ska vara Post- och telestyrelsen till handa inom två veckor från det att den inledande rapporten lämnades. Anstånd kan beviljas.

Rapporten ska innehålla uppgifter om

1. komplettering och uppdatering av uppgifterna som lämnats i den inledande rapporten,
2. orsakerna till säkerhetsincidenten,
3. vilken information som har lämnats till allmänheten och berörda personer samt vid vilken tidpunkt och på vilket sätt denna information lämnades,
4. de åtgärder som har vidtagits för att minimera effekterna av säkerhetsincidenten inför slutligt avhjälpande,
5. de åtgärder som har vidtagits för att avhjälpa de fel och brister som orsakat säkerhetsincidenten och vid vilken tidpunkt åtgärderna vidtogs,
6. de åtgärder som har vidtagits och som planeras för att undvika liknande säkerhetsincidenter samt vid vilken tidpunkt dessa åtgärder vidtogs eller när de bedöms vara genomförda, och
7. referensnummer för ärendet.

Allmänt råd till 4 §

Tillhandahållarens redogörelse för orsakerna till säkerhetsincidenten bör beskriva samtliga kända omständigheter som har eller kan ha bidragit till att incidenten inträffade.

Tröskelvärden för rapportering

5 § En säkerhetsincident som innebär störning eller avbrott i tillhandahållna kommunikationsnät eller kommunikationstjänster ska rapporteras under följande förutsättningar.

Tid som incidenten pågått	*Incidentens uppskattade omfattning*
≥ 1 timme	≥ 150 000 användare eller aktiva anslutningar i Sverige, ≥ 50 procent kapacitetsbortfall eller ≥ 15 000 km² sammanhängande berört område
≥ 2 timmar	≥ 30 000 användare eller aktiva anslutningar i Sverige, ≥ 30 procent kapacitetsbortfall eller ≥ 5 000 km² sammanhängande berört område
≥ 6 timmar	≥ 5 000 användare eller aktiva anslutningar i Sverige, ≥ 20 procent kapacitetsbortfall eller ≥ 2 500 km² sammanhängande berört område
≥ 24 timmar	≥ 2 000 användare eller aktiva anslutningar i Sverige, ≥ 10 procent kapacitetsbortfall eller ≥ 1 000 km² sammanhängande berört område

Allmänt råd till 5 §
Berört område för kommunikationstjänster som tillhandahålls över mobila nätanslutningar bör normalt vara det sammanlagda täckningsområdet för berörda celler eller motsvarande i mobilnätet.

Kapacitetsbortfall bör till exempel kunna beräknas som andelen berörda användare eller aktiva anslutningar i förhållande till det totala antalet användare eller aktiva anslutningar för kommunikationstjänsten, eller, andel misslyckade samtalsförsök.

6 § Utöver vad som framgår av 5 § ska en säkerhetsincident rapporteras om den på annat sätt har haft en betydande påverkan på kommunikationsnätet eller kommunikationstjänsten eller betydande påverkan på funktioner i samhället.

Integritetsincidenter

7 § Bestämmelser om rapportering av integritetsincidenter finns i 8 kap. 8 § lagen (2022:482) om elektronisk kommunikation och kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation.

---

1. Dessa föreskrifter träder i kraft den 1 augusti 2022.
2. Genom föreskrifterna upphävs
a) Post- och telestyrelsens föreskrifter (PTSFS 1995:1) om fredstida planering för totalförsvarets behov av telekommunikation m.m.
b) Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2012:2) om rapportering av störningar eller avbrott av betydande omfattning,
c) Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2012:4) om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,
d) Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter,
e) Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet.

På Post- och telestyrelsens vägnar

DAN SJÖBLOM

Karolina Asp