Post- och telestyrelsens författningssamling

Utgivare: Karolina Asp, Post- och telestyrelsen, Box 5398, 102 49 Stockholm
ISSN 1400-187X

Post- och telestyrelsens föreskrifter om krav på driftsäkerhet;

PTSFS 2015:2

Utkom från trycket
den 22 juni 2015

beslutade den 10 juni 2015.

Med stöd av 30 § förordningen (2003:396) om elektronisk kommunikation föreskriver Post- och telestyrelsen följande.

Tillämpningsområde och definitioner

1 § Dessa föreskrifter innehåller bestämmelser om de tekniska och organisatoriska åtgärder som den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta enligt 5 kap. 6 b § lagen (2003:389) om elektronisk kommunikation.

2 § I dessa föreskrifter avses med

aktiv anslutning: anslutning till kommunikationsnät eller kommunikationstjänst som möjliggör omedelbar användning av 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,

GSM: Global System for Mobile Telecommunications,

incident: händelse som orsakar eller inom kort kan orsaka störning eller avbrott i kommunikationstjänst eller kommunikationsnät,

kommunikationsnät: allmänt kommunikationsnät i enlighet med 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation,

kommunikationstjänst: elektronisk kommunikationstjänst, i enlighet med 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation, som är allmänt tillgänglig,

kontrollfunktion för basstationer: tillgång i mobila kommunikationsnät som kontrollerar en eller flera basstationer för GSM (Base Station Controller) eller basstationer (node B) för UMTS (Radio Network Controller), i enlighet med definitionerna i specifikation 3GPP, utgåva 13.1.0[1],

[1] Technical Specification Group Services and System Aspects; Network architecture, 3GPP TS 23.002 V13.1.0 (2014-12). Specifikationen publiceras av 3rd Generation Partnership Project och finns tillgänglig på 3GPP:s webbplats, www.3gpp.org.

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

kritisk verksamhetsdel: del av verksamheten som är nödvändig för att kunna begränsa omfattande störningar eller avbrott i kommunikationsnät och kommunikationstjänster,

redundanta förbindelser: två eller flera, identiska eller olika, förbindelser som oberoende av varandra fyller samma funktion,

redundanta kritiska komponenter: två eller flera, identiska eller olika, kritiska komponenter som oberoende av varandra fyller samma funktion,

redundanta tillgångar: två eller flera, identiska eller olika, tillgångar som oberoende av varandra fyller samma funktion,

reservkraftssystem: 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 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: aktör som tillhandahåller kommunikationsnät eller kommunikationstjänster,

UMTS: Universal Mobile Telecommunications System,

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

Övergripande driftsäkerhetsarbete

3 § Tillhandahållarens driftsäkerhetsarbete ska bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala driftsförhållanden som extraordinära händelser.

Tillhandahållaren ska i driftsäkerhetsarbetet ha en tydlig rollfördelning med särskilt utpekade ansvariga för arbetet.

Tillhandahållaren ska ta fram och dokumentera de processer, planer och tester som föreskrivs i 5, 7, 8, 12, 13, 21 och 22 §§ samt säkerställa att anställda och uppdragstagare har kunskap om de processer och planer som de är berörda av.

Tillhandahållaren ska dokumentera de åtgärder som vidtas enligt 10-12 §§ och 16-22 §§ samt följa upp dessa åtgärder årligen och vid behov.

Dokumentation av tillgångar och förbindelser

4 § Tillhandahållaren ska dokumentera samtliga sina tillgångar och förbindelser.

Tillhandahållaren ska för respektive tillgång och förbindelse åtminstone dokumentera

1. en unik beteckning,
2. vilken funktionalitet tillgången eller förbindelsen har,

3. tillgångens eller förbindelsens geografiska placering,
4. en hänvisning till den för tillgången eller förbindelsen aktuella riskanalysen enligt 5 §, och
5. tillgångens klass enligt 15 §.

Dokumentationen enligt första och andra stycket ska hållas uppdaterad.

Riskanalys och konsekvensanalys

5 § Tillhandahållaren ska minst en gång per år analysera risken för att dokumenterade tillgångar och förbindelser enligt 4 § orsakar störningar eller avbrott i de kommunikationsnät och kommunikationstjänster som denne tillhandahåller.

Tillhandahållaren ska, utöver vad som föreskrivs i första stycket, genomföra riskanalyser inför sådana planerade förändringar som kan påverka driftsäkerheten i de kommunikationsnät och kommunikationstjänster som denne tillhandahåller, samt efter att sådana störningar eller avbrott som ska rapporteras enligt 5 kap. 6 c § lagen (2003:389) om elektronisk kommunikation har inträffat.

Riskanalyserna enligt första och andra stycket ska innefatta åtminstone följande delar:

1. Identifiering av samtliga relevanta hot mot den aktuella tillgången eller förbindelsen. Hot relaterade till väder samt intrång och annan yttre påverkan ska alltid analyseras.
2. Kvalificerad bedömning av konsekvenser i händelse av att identifierade hot inträffar.
3. Kvalificerad bedömning av sannolikheten för att identifierade hot inträffar.
4. Kvalificerad sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de inträffar (riskbedömning).

Vid genomförande av riskanalyser ska tillhandahållaren beakta erfarenheter från inträffade incidenter samt tillämpa processer som utgår från etablerad standard på området.

Tillhandahållaren ska ha en plan för vid vilka tidpunkter och i vilka situationer tillhandahållaren kommer att genomföra riskanalyser.

Tillhandahållaren ska dokumentera genomförda riskanalyser.

6 § Tillhandahållaren ska analysera vilka konsekvenser som kan uppstå när kritiska verksamhetsdelar helt eller delvis upphör att fungera. Analysen ska omfatta en bedömning av när särskilda handlingsplaner enligt 8 § ska tillämpas.

Konsekvensanalysen enligt första stycket ska dokumenteras och revideras vid behov.

Planering för och hantering av inträffade händelser som kan orsaka störningar eller avbrott

7 § Tillhandahållaren ska säkerställa att

1. inträffade incidenter rapporteras internt,
2. åtgärder vidtas skyndsamt för att hantera en uppkommen incident,
3. åtgärder vidtas för att undvika liknande incidenter, och
4. att erfarenheter från inträffade incidenter beaktas vid genomförande av riskanalyser enligt 5 §.

Vid vidtagande av åtgärder enligt första stycket (incidenthantering) ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

8 § Tillhandahållaren ska tillämpa särskilda handlingsplaner i enlighet med sin analys och bedömning enligt 6 §. Handlingsplanerna ska innefatta åtgärder för att begränsa de konsekvenser som kan uppstå enligt analysen samt för att återställa kritiska verksamhetsdelar till normal funktionsförmåga (kontinuitetsplanering).

Tillhandahållaren ska utgå från etablerad standard på området vid framtagande av handlingsplanerna. Tillhandahållaren ska revidera handlingsplanerna vid behov och öva planerna vartannat år.

Åtgärder efter riskbedömning

9 § Tillhandahållaren ska vidta de åtgärder som föreskrivs i 10-12 §§, samt de ytterligare åtgärder som är nödvändiga med hänsyn till den risk för störning eller avbrott som framkommit i tillhandahållarens riskbedömning enligt 5 §. Samtliga åtgärder ska vidtas på den nivå som är proportionerlig med hänsyn till riskbedömningen, de kostnader som är förenade med åtgärden samt verksamhetens art och omfattning.

Tillhandahållarens bedömning av nivå enligt första stycket ska dokumenteras och följas upp årligen och vid behov.

Intrång och annan yttre påverkan

10 § Tillhandahållaren ska vidta åtgärder för att skydda tillgångar mot fysiska och logiska intrång och annan yttre påverkan.

Väderrelaterade hot

11 § Tillhandahållaren ska vidta åtgärder för att skydda tillgångar och förbindelser mot nederbörd, vind, blixtnedslag, fukt, skadliga temperaturer, översvämningar, jordskred och brand.

Planerade förändringar

12 § Innan tillhandahållaren genomför förändringar i sina kommunikationsnät och kommunikationstjänster som kan orsaka sådana störningar eller avbrott som ska rapporteras enligt 5 kap. 6 c § lagen (2003:389) om elektronisk kommunikation, ska tillhandahållaren säkerställa att tester utförs. Tillhandahållaren ska planera för att återställa kommunikationsnätet och kommunikationstjänsten i händelse av att störning

eller avbrott inträffar. Tester 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.

Åtgärder avseende åtkomst och behörighet

13 § Tillhandahållaren ska medge åtkomst till sina tillgångar endast till den som är behörig. Tillhandahållaren ska tilldela sådan behörighet endast till den 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 och följas upp årligen och vid behov.

Åtgärder avseende övervakning och beredskap

14 § Tillhandahållaren ska ha system som kontinuerligt övervakar kommunikationstjänster och aktiva delar i tillhandahållarens kommunikationsnät. Systemen ska generera larm vid störningar eller avbrott. Tillhandahållaren ska ha beredskap dygnet runt för att ta emot larm och initiera relevanta åtgärder.

Klassificering av tillgångar

15 § Tillgångar indelas i följande fem klasser utifrån det antal aktiva anslutningar som kan omfattas av 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

Åtgärder efter klassificering av tillgångar

Redundans av tillgångar i klasserna A och B

16 § 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. Sådan störning eller avbrott som består i att sessioner avbryts är dock tillåten, om användare omedelbart kan upprätta nya sessioner.

Första stycket gäller inte tillgångar i klasserna A och B som utgörs av kontrollfunktioner för basstationer.

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

Redundans av tillgångar i klass C

17 § 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. Sådan störning eller avbrott som består i att sessioner avbryts är dock tillåten, om användare omedelbart kan upprätta nya sessioner.

Säkerställande av tillgångar i klass D

18 § 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

19 § 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. Sådan störning eller avbrott som består i att sessioner avbryts är dock tillåten, 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

20 § 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.

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

21 § Tillhandahållaren ska med reservkraftssystem säkerställa att fel i extern elförsörjning inte orsakar störning eller avbrott i de kommunikationsnät och kommunikationstjänster som denne tillhandahåller, 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, från det att felet i den externa elförsörjningen inträffade.

Fel i extern elförsörjning som inträffar med mindre än 4 timmars mellanrum avseende samma tillgång ska anses utgöra 1 fel.

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

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

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

Reservkraftssystem avseende mobila kommunikationstjänster och mobila kommunikationsnät

22 § Tillhandahållare av mobila kommunikationsnät och mobila kommunikationstjänster ska med reservkraftssystem, utöver vad som följer av 21 §, säkerställa att fel i extern elförsörjning inte orsakar störning eller avbrott i kommunikationsnät och kommunikationstjänster som denne tillhandahåller eller minskar kommunikationstjänsters täckningsområde, under åtminstone 1 timme i tätort med fler än 8 000 invånare och 4 timmar på övriga platser, från det att felet i extern elförsörjning inträffade. Fel i extern elförsörjning som inträffar med mindre än 4 timmars mellanrum avseende samma tillgång ska anses utgöra 1 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. Om kvarvarande frekvensband inte ger tillräcklig kapacitet för att upprätthålla samtliga tillhandahållarens kommunikationstjänster, får tillhandahållaren fördela kapaciteten så att i första hand samtalstjänst, i andra hand meddelandetjänst och i tredje hand datakommunikationstjänst tillhandahålls.

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

Ansökan om undantag avseende 16-22 §§

23 § Post- och telestyrelsen kan efter ansökan från en tillhandahållare medge undantag från kraven i 16-22 §§ i följande fall.

1. Tillgänglig teknik, kostnader förenade med åtgärden och tillhandahållarens riskbedömning enligt 5 § sammantaget medför att åtgärden är olämplig i förhållande till de positiva effekter för driftsäkerheten som den medför och tillhandahållaren vidtar

lämpliga alternativa åtgärder när sådana finns.

2. Annan reglering förhindrar vidtagandet av åtgärden.
3. Tillgänglig teknik, kostnader förenade med åtgärden och tillhandahållarens riskbedömning enligt 5 § sammantaget medför att åtgärden är olämplig i förhållande till att åtgärden avser tillgångar eller förbindelser som omfattas av beslut om avveckling och tillhandahållaren vidtar lämpliga alternativa åtgärder när sådana finns.

Utöver vad som föreskrivs i första stycket punkterna 1-3 måste tillhandahållaren i samtliga fall även redovisa vilka alternativa åtgärder som denne har för avsikt att vidta för att begränsa negativa effekter av att den föreskrivna åtgärden inte vidtas, samt vilken påverkan på driftsäkerheten som detta medför.

---

1. Denna författning träder i kraft,
   a. 5 år efter den dag då författningen beslutades i fråga om
      i. åtgärder enligt 16 - 20 §§, avseende den 1 januari 2016 befintliga tillgångar i klasserna A-D, så länge tillhandahållaren inte genomför förändringar av tillgången,
      ii. åtgärder enligt 21 och 22 §§, avseende den 1 januari 2016 befintliga reservkraftssystem för tillgångar i klasserna A-D respektive i mobila kommunikationsnät, så länge tillhandahållaren inte genomför förändringar av tillgången eller reservkraftssystemet, och
   b. den 1 januari 2016 i övrigt.
2. Genom författningen upphävs Post- och telestyrelsens allmänna råd (PTSFS 2007:2) om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid.

På Post- och telestyrelsens vägnar

GÖRAN MARBY

Karolina Asp