

Föreskrifter om ändring i Post- och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet;

PTSFS 2020:1

Utkom från trycket
den 25 februari 2020

beslutade den 20 februari 2020.

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

dels att 2, 4—5, 9—10 och 13 §§ samt rubrikerna närmast före 4 och 10 §§ ska ha följande lydelse,

dels att det i föreskrifterna ska införas fyra nya paragrafer, 4 a, 5 a, 9 a och 11 a §§, samt närmast före 9 a och 11 a §§ nya rubriker av följande lydelse.

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 13.1.011,

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,

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.

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,

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

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

Dokumentation av tillgångar, förbindelser och uppdragstagare

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 §,
5. tillgångens eller förbindelsens tillverkare, och
6. tillgångens klass enligt 15 §.

Dokumentationen enligt första och andra stycket ska hållas uppdaterad och bevaras i fem år från det att den upprättats eller uppdaterats.

4 a § Tillhandahållaren ska dokumentera samtliga uppdragstagare.

Dokumentationen ska åtminstone innehålla

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

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

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, intrång, sabotage och annan yttre påverkan ska alltid analyseras, liksom sådan information som förmedlas från Post- och telestyrelsen om hot.
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.

5 a § Tillhandahållaren ska inför upphandling av tillgångar, förbindelser eller uppdragstagare genomföra och dokumentera en sådan analys som föreskrivs i 5 §.

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 och 5 a §§. 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.

Information om hot

9 a § Tillhandahållaren ska vidta åtgärder för att hantera risker som framkommit efter analys av information som förmedlats från Post- och telestyrelsen om hot.

Intrång, sabotage och annan yttre påverkan

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

Upphandling

11 a § Tillhandahållaren ska vidta åtgärder för att hantera risker som identifierats vid riskanalys enligt 5 a §.

13 § Tillhandahållaren ska medge åtkomst till sina tillgångar 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 och följas upp årligen samt vid behov.

Dessa föreskrifter träder i kraft den 1 mars 2020.

På Post- och telestyrelsens vägnar

DAN SJÖBLOM

Karolina Asp