Utfärdad:	Träder i kraft:	Giltighetstid:
[dd.mm.åååå]	[dd.mm.åååå]	tills vidare

Rättsgrund
Lag om tjänster inom elektronisk kommunikation (917/2014) 244, 247 och 272 §

Bestämmelser om påföljderna för verksamhet som strider mot föreskriften finns i
lagen om tjänster inom elektronisk kommunikation (917/2014) 330–332, 340 och 349 §

EU-lagstiftning som ska verkställas:
Europaparlamentets och rådets direktiv (EU) 2018/1972, artikel 40
Europaparlamentets och rådets direktiv 2002/58/EG, artikel 4

Ändringsuppgifter:
Upphäver Kommunikationsverkets föreskrift om televerksamhetens informationssäkerhet 67 A/2015 M som utfärdades 4.3.2015.

Föreskrift om televerksamhetens informationssäkerhet

Innehåll

Kapitel 1 Tillämpningsområde och definitioner

1 Tillämpningsområde

1. Denna föreskrift tillämpas på allmän televerksamhet.

2. Punkt 15.1 i föreskriften tillämpas också på kommunikationstjänster som anknyter till myndighetsnät och myndighetskommunikation till den del de är sammankopplade med ett allmänt kommunikationsnät eller en allmänt tillgänglig kommunikationstjänst.

3. I denna föreskrift fastställs
   - i kapitel 2 om informationssäkerhetsåtgärder i alla allmänna kommunikationsnät och i allmänt tillgängliga kommunikationstjänster
   - i kapitel 3 om särskilda krav på gränssnitt
   - i kapitel 4 om särskilda krav på internetaccesstjänster
   - i kapitel 5 om särskilda krav på tjänster för text- och multimediemeddelanden, och
   - i kapitel 6 om särskilda krav på e-posttjänster.

2 Definitioner

1. I denna föreskrift avses med

   1) *kundgränssnitt* ett gränssnitt genom vilket ett kommunikationsnät, en terminalutrustning eller en applikation för teleföretagets kund kopplas till det allmänna kommunikationsnätet,

   2) *öppen proxyserver för e-post* ett sådant meddelandeförmedlingssystem för e-post som tredje part obehörigt kan använda för förmedling av e-postmeddelanden,

   3) *skadlig trafik* elektroniska meddelanden som (a) utgör ett hot mot informationssäkerheten i kommunikationsnäten eller mot i dessa anknutna tjänster och datasystem, (b) mot vilka åtgärder kan riktas på det sätt som avses i 272 § 1 mom. 2 punkten i lagen om tjänster inom elektronisk kommunikation för att trygga kommunikationsmöjligheterna för den som sänder eller tar emot meddelanden, eller som (c) via kommunikationstjänsterna används för sådana omfattande förberedelser för betalningsbedrägeri som nämns i 37 kap. 11 § i strafflagen,

   4) *filtrering* förhindrande eller begränsning av skadlig trafik, avlägsnande av sådana skadliga datorprogram ur elektroniska meddelanden som kan äventyra informationssäkerheten, eller andra åtgärder av teknisk natur som är jämförbara med dessa, inklusive omnämnande om att meddelandet är skadlig trafik,

   5) *e-posttjänst* en tjänst för sändning, förmedling eller mottagning av e-postmeddelanden, som utnyttjar domännamnssystemet för att förmedla meddelanden,

   6) *komponent i kommunikationsnätet eller -tjänsten* ett nätelement, en utrustning eller ett datasystem som kommunikationsnätet eller -tjänsten består av eller utnyttjar,

   7) *samtrafikgränssnitt* det gränssnitt där teleföretagens kommunikationsnät eller -tjänster kopplas samman,

   8) *textmeddelandetjänst* förmedlingstjänst för korta meddelanden genom förmedling via mobilnätets meddelandecentraler, och

9) *tjänster för multimediemeddelanden* en förmedlingstjänst av korta meddelanden som innehåller multimedia såsom bilder, ljud, videor och redigerad text via mobilnätets centraler för multimedia.

2. Därutöver används i denna föreskrift definitioner som anges i 3 § i lagen om tjänster inom elektronisk kommunikation (917/2014).

Kapitel 2 Allmänna krav på informationssäkerhet

3 Hänsynstagande till informationssäkerheten

1. Ett teleföretag ska i de olika skedena av kommunikationsnätens och -tjänsternas livscykel beakta följande:

   1) informationssäkerhet och riskhantering,

   2) personalsäkerhet,

   3) säkerhet inom informationssystem och telekommunikationsområdet samt fysisk säkerhet,

   4) informationssäker funktion och ändringshantering,

   5) upptäckt och hantering av situationer som hotar eller stör informationssäkerheten,

   6) driftskontinuitetshantering,

   7) observation, testning och bedömning av informationssäkerheten, och

   8) medvetenheten om hot samt information till abonnenter och användare.

2. Teleföretag ska dokumentera och svara för en aktuell beskrivning av hur företaget i sin verksamhet genomför de faktorer som nämns i första punkten och övriga krav som nämns i detta kapitel.

4 Hantering av informationssäkerhet och risker

1. Teleföretagen ska ägna uppmärksamhet åt hanteringen av informationssäkerhet och risker genom att åtminstone uppfylla följande krav:

   1) Teleföretagen ska ha en ändamålsenlig informationssäkerhetspolicy och verksamhetsprinciper som preciserar policyn, som de regelbundet ska upprätthålla med beaktande av åtminstone förändringar i verksamhetsmiljön, observerade avvikelser, övningar samt förutsebara förändringar i informationssäkerhetens hotmiljö.

   2) Teleföretag ska identifiera de funktioner, data och system som är viktiga för televerksamhetens kontinuitet samt i form av en kontinuerlig process bedöma och behandla informationssäkerhetsriskerna som riktas mot dessa. Särskild uppmärksamhet ska ägnas åt bedömningen av riskerna som gäller leveranskedjorna, virtualiseringsmiljöerna och Edge Computing-enheterna.

   3) Teleföretag ska fastställa ändamålsenliga informationssäkerhetsroller och informationssäkerhetsansvar i överensstämmelse med informationssäkerhetspolicyn och verksamhetsprinciperna som preciserar den. Teleföretag ska förhindra uppkomsten av ansvars- och uppgiftshelheter som äventyrar informationssäkerheten eller, om detta inte är möjligt, på annat sätt hantera de risker som dessa medför.

4) Teleföretag ska fastställa ändamålsenliga informationssäkerhetskrav på leverantörsförhållanden och leverantörsavtal och utarbeta specificerade verksamhetsprinciper och riskhanteringsprocesser med vilka kommunikationsnätens och -tjänsternas informationssäkerhet i hela leverantörskedjan kan säkerställas.

2. Resultaten från riskhanteringsprocessen, som anges i första punkten andra strecksatsen ovan, ska sparas åtminstone i tre år eller räknat från de tre sista behandlingarna, beroende på vilken tid för sparandet är längre.

5 Personalsäkerhet

Teleföretag ska uppmärksamma personalsäkerheten genom att åtminstone uppfylla följande krav:

1) Teleföretag ska genomföra nödvändiga utredningar av sin personal för att säkerställa att den är tillförlitlig i de fall då det med avseende på en persons uppgift och ansvar är nödvändigt.

2) Teleföretag ska se till att personalen har tillräckliga kunskaper i informationssäkerhet, och att kurser i informationssäkerhet ordnas regelbundet för att upprätthålla personalens kompetens. Teleföretag ska se till att personalen känner till informationssäkerhetspolicyn och verksamhetsprinciper som avses i punkt 4.1.1 i föreskriften, målen för dessa och konsekvenserna i relation till deras egna arbetsuppgifter.

3) Teleföretag ska ha ändamålsenliga tillvägagångssätt för att kunna hantera informationssäkerhetsrisker som förändringar inom personalen eller personalens uppgifter medför.

4) Teleföretag ska ha ändamålsenliga tillvägagångssätt för att kunna följa verksamhetsprinciperna och förfaranden som gäller informationssäkerhet för att kunna ingripa i avvikelser till följd av personalens verksamhet och för att kunna hantera informationssäkerhetskränkningar till följd av personalens verksamhet.

6 Säkerhet inom informationssystem och telekommunikationsområdet samt fysisk säkerhet

1. Teleföretag ska uppmärksamma säkerheten inom informationssystem och telekommunikationsområdet genom att åtminstone uppfylla följande krav:

1) För att få tillgång till teleföretagens kommunikationsnät och informationssystem och för administrering av behörigheter ska ändamålsenliga förfaranden som upprätthålls enligt riktade verksamhetsprinciper för åtkomstkontroll användas.

2) Teleföretag ska sköta om integriteten hos kommunikationsnäten och -tjänsterna, terminalerna och informationssystemen som personalen använder och skydda dessa mot tillägg av skadliga koder och skadlig programvara som kan tänkas ändra funktionerna i systemen.

3) Teleföretag ska skydda de system som är centrala för kommunikationsnäten och -tjänsterna mot överbelastningsangrepp. Skyddsåtgärderna ska dimensioneras i enlighet med en aktuell riskbedömning.

4) Teleföretag ska ha riktade verksamhetsprinciper och ändamålsenliga förfaranden för kryptografi och användning av kryptering under den tid som förmedlingsuppgifter, meddelanden, platsinformation, styrtrafik och teleföretagens datamaterial som an-

vänds för televerksamheten lagras och överförs. Med tanke på informationssäkerhetsrisken ska i verksamhetsprinciperna åtminstone datamaterial och trafikhändelser som kräver kryptering definieras, likaså krypteringsteknik och krypteringsförfaranden som används, förvaltning av krypteringsnycklar och undantag i fråga om krypteringspraxis. Teleföretag ska använda ändamålsenlig kryptering alltid när det är tekniskt möjligt och ändamålsenligt i förhållande till informationssäkerhetsrisker avseende lagring eller överföring och kostnaderna för kryptering.

5) Teleföretag ska ha ändamålsenliga verksamhetsprinciper och förfaranden för att skydda och behandla hemliga uppgifter i krypteringsnyckelmaterialen och hemliga uppgifter som används vid autentisering.

6) Komponenterna i kommunikationsnät och -tjänster som genomförts i en virtualiseringsmiljö ska genomföras så att man endast tillåter funktioner och behörigheter som är nödvändiga för att de ska fungera.

2. Teleföretagen ska ha ändamålsenliga verksamhetsprinciper och förfaranden för skötseln av den fysiska säkerheten i informationssystemen, utrustningen, informationsmaterialen och lokaler samt för utrustningens miljöförhållanden. Om fysiskt skydd av utrustningsutrymmen föreskrivs även i Transport- och kommunikationsverkets föreskrift om säkerställande av kommunikationsnät och -tjänster samt om synkronisering av kommunikationsnät.

7 Informationssäker funktion och ändringshantering

1. Teleföretag ska genomföra funktionen och förändringshanteringen för kommunikationsnäten och -tjänsterna så att teleföretagen åtminstone beaktar följande krav i dessa:

   1) Teleföretag ska ha ändamålsenliga verksamhetsprinciper och förfaranden för bruket av komponenter i kommunikationsnätet eller -tjänsten.

   2) Teleföretag ska ha ändamålsenliga ändringsförfaranden med hjälp av vilka man minskar sannolikheten för störningar i informationssäkerheten på grund av förändringar, eller vid behov återställer det läge som föregick ändringen eller något annat fungerande läge.

   3) Teleföretaget ska ha ändamålsenliga verksamhetsprinciper och förfaranden för hanteringen av egendom och konfigurationer.

2. Om ändringshantering föreskrivs även i 9 § i Transport- och kommunikationsverkets föreskrift om störningar i televerksamheten.

8 Testning och bedömning av informationssäkerheten

Teleföretag ska genomföra testning och bedömning av informationssäkerheten i kommunikationsnät och -tjänster så att åtminstone följande krav beaktas:

1) Teleföretag ska ha ändamålsenliga verksamhetsprinciper och förfaranden för testning av informationssäkerheten hos komponenter i kommunikationsnät och -tjänster och vid behov enligt riskbedömning för utförande av säkerhetsbedömningar av dem.

2) Ett teleföretag ska ha ändamålsenliga verksamhetsprinciper och förfaranden för att följa upp hur dess informationssäkerhetspolicy och verksamhetsprinciper samt de krav på informationssäkerhet som hänför sig till verksamheten uppfylls (bedömning av informationssäkerhet). Resultaten av åtminstone den senaste bedömningen ska bevaras.

9 Medvetenhet om hot

Teleföretag ska ha ändamålsenliga tillvägagångssätt för att samla in uppgifter om hot och för bedömning av hot som gäller kommunikationsnätens och -tjänsternas informationssäkerhet.

10 Iakttagande av standarder

1. Mobilnätverkets teleföretag ska ha ändamålsenliga tillvägagångssätt med hjälp av vilka säkerhetskraven i de tekniska normerna (standarder) som anges i bilaga 1 uppfylls med LTE-teknik i fjärde generationens mobilnät, femte generationens mobilnät och IP-baserade allmänna telefontjänster. Av standarderna ska den nyaste versionen användas, dvs. den som är godkänd av 3GPP och som motsvarar de funktioner som teleföretagen genomför i sina kommunikationsnät och -tjänster.

2. Teleföretag kan låta bli att uppfylla det säkerhetskrav som anges i första punkten, i det fall att det inte är ändamålsenligt med beaktande av dess betydelse för kommunikationsnätets eller -tjänstens informationssäkerhet och övriga till saken anknutna åtgärder för att ombesörja informationssäkerheten i det aktuella fallet.

3. Teleföretag ska upprätthålla en beskrivning om hur de i sin verksamhet beaktar vad som föreskrivs i första stycket. Varför säkerhetsåtgärden eller mekanismen inte utförts utgående ifrån den andra punkten och motiveringarna till varför åtgärderna inte vidtagits ska dokumenteras specifikt för respektive säkerhetskrav.

11 Datamaterial

Teleföretag ska ha ett klassificeringssystem, klassificeringskriterier och hanteringsförfaranden i samband med klassificeringen av sådant datamaterial som är viktigt för televerksamheten.

12 Identifiering av kund i syfte att sköta om informationssäkerheten

Teleföretag ska ha ändamålsenliga verksamhetsprinciper och tillvägagångssätt för att kunna identifiera abonnenten eller användaren på ett tillräckligt tillförlitligt sätt med tanke på risknivån i skötseln av ärenden innan ändringar som påverkar kommunikationstjänsten informationssäkerhet utförs på kundens tjänst eller innan abonnenten eller användaren ges konfidentiella uppgifter.

13 Dokumentation av IP-adresser

Teleföretag ska se till att de IP-adresser som är adresserade till teleföretaget och som annonseras av teleföretaget är dokumenterade på behörigt sätt i databasen för den internet-registrator som tilldelat adressrymden eller någon annan ändamålsenlig internet-registrator.

14 Trafik mellan hanteringsnät och hanteringsförbindelser

1. Teleföretag ska ha ändamålsenliga verksamhetsprinciper och praxis vad beträffar nätverksadministration och administrationsförbindelser.

2. Teleföretag ska på ett ändamålsenligt sätt skydda och vid behov kryptera kontrolltrafiken av komponenter i kommunikationsnätet eller -tjänsten så att obehöriga ändringar av komponenterna i kommunikationsnätet eller -tjänsten är förhindrade enligt verksamhetsprinciperna.

3. Teleföretag ska ha ändamålsenliga förfaranden för att bedöma hot mot informationssäkerheten som orsakas av terminaler som används för nätverksadministration och för att hantera risker orsakade av dessa.

Kapitel 3 Särskilda krav på kommunikationsnät och -tjänsternas gränssnitt

15 Förhindrande av och skydd mot störningar i gränssnitten

1. Teleföretag ska se till att komponenterna i dess kommunikationsnät eller -tjänster inte orsakar störningar för övriga kommunikationsnät eller -tjänster. Teleföretaget ska ha ändamålsenliga mekanismer för att förhindra sådana störningar.

2. Företaget ska skydda sina kommunikationsnät och -tjänster mot skadlig trafik från samtrafik-, tillämpnings- och kundgränssnitt genom att genomföra nödvändiga skyddsmekanismer i sina nät.

16 Stängning av onödiga portar, tjänster och protokoll

Teleföretag ska se till att kommunikationsnätets eller -tjänstens komponenter eller portar som finns i teleföretagets samtrafik- och kundgränssnitt inte har onödiga tjänster eller protokoll påslagna.

17 Skydd av IP-samtrafikgränssnitt och filtrering av trafiken

1. För att skydda sina IP-samtrafikgränssnitt ska teleföretagen åtminstone se till följande:

    1) upptäcka avvikelser i routningen,

    2) skydda uppkopplingar som används för att ändra routinguppgifter alltid när det är möjligt,

    3) filtrera trafik som innehåller felaktig IP-källadress och som riktas till de egna kommunikationsnäten, inberäknat trafik där källadressen för mottaget IP-paket

        i) hör till den IP-adressrymd som teleföretaget själv administrerar eller annonserar eller den IP-adressrymd som är reserverad för icke-offentligt bruk eller som

        ii) inte hör till rutter som annonseras av ett teleföretag som förmedlar trafik till andra teleföretag,

    4) avvisa sådana rutter från mottagna ruttannonseringar

        i) som hör till teleföretagets egna adressblock eller till sådana adressblock som teleföretaget levererar till kunden och som inte kan förväntas bli annonserade av andra teleföretag och

        ii) ruttannonseringar med felaktig ROA-poster (Route Origin Authorization), samt

    5) skapa ROA-poster för de nätområden de förvaltar om det är tekniskt möjligt, och se till att de undertecknas och publiceras.

2. Den trafik som nämns i första punkten tredje strecksatsen kan dock förmedlas, och ruttannonserna som beskrivs i fjärde strecksatsen kan för enskilda nät tillåtas, om aktörerna avtalat om detta separat.

18 Förhindrande av förfalskning av källadress i kundgränssnitt i IP-trafiken

1. Teleföretag ska filtrera sådan trafik från ett kundabonnemang till kommunikationsnätet vars källadress inte är anvisad vederbörande kundabonnemang. Teleföretaget ska genomföra filtreringen i det nätelement som befinner sig närmast kundgränssnittet och där det tekniskt sett är mest ändamålsenligt att göra filtreringen.

2. En lindrigare åtgärd än sådan filtrering av trafik som avses ovan i första punkten är att teleföretaget kontaktar kunden för att utreda situationen som äventyrar informationssäkerheten.

19 Skydd av gränssnitt i mobilnätet

Teleföretag ska skydda gränssnitten i sina mobilnät för att säkerställa kommunikationsnätets och -tjänstens informationssäkerhet och för att förhindra obehörig omstyrning av trafiken. Teleföretag ska i mobilnätets gränssnitt åtminstone göra följande:

1) övervaka signaleringsgränssnittens informationssäkerhet och planera, genomföra och upprätthålla åtgärder för att kunna hantera signaleringsgränssnittens informationssäkerhet. Hanteringsåtgärderna ska basera sig på vetskap om hot och riskbedömning,

2) skydda mobilnätverksskivans hanteringsförbindelse på ett sådant sätt att bara auktoriserade parter kan skapa, ändra eller radera skivan eller få information om skivans egenskaper, abonnenter eller användare,

3) utöver primär autentisering av mobilnätet även utföra skivspecificerad bekräftelse av behörigheten hos och auktorisering av terminalerna där andra autentiseringsuppgifter än de som används vid primär autentisering används om det, med beaktande av informationssäkerhetshot och tekniska möjligheter avseende användning av den ifrågavarande skivan, är nödvändigt att bekräfta behörighet och genomföra autentisering, samt

4) genomföra nödvändiga skyddsmekanismer i nätet och därigenom skydda kommunikationsnätet och -tjänsterna mot skadlig trafik som en Edge Computing-enhet eventuellt riktar mot dessa.

Kapitel 4 Särskilda krav för internetaccesstjänster

20 Åtskiljande av trafik i internetaccesstjänster

1. Teleföretag ska skilja kundabonnemangens trafik från varandra så att användarna av de olika kundabonnemangen inte obehörigt kan följa med varandras trafik. Teleföretaget ska säkerställa att det inte är möjligt att obehörigen omdirigera trafik mellan abonnemangen.

2. Oberoende av vad som anges i första punkten, kan teleföretaget tillhandahålla okrypterade WLAN-förbindelser utan att åtskilja trafiken i radiogränssnittet.

21 Dirigering av e-posttrafik från konsumentabonnemang

1. Teleföretag ska förhindra obegränsad SMTP-trafik från konsumentabonnemang om det sker på andra sätt än via överenskomna servrar avsedda för den utgående SMTP-trafiken.

2. Oberoende av vad som anges i första punkten kan teleföretaget tillåta obegränsad SMTP-trafik även på andra sätt än via överenskomna servrar avsedda för den utgående SMTP-trafiken. Då måste teleföretaget underrätta abonnenten om de risker som hänför sig till öppen trafik. Teleföretag ska även ha beredskap att snabbt reagera på störningar.

22 Skyldighet att filtrera skadlig trafik i internetaccesstjänster

1. Teleföretag ska ha behövliga system och tillvägagångssätt att tillfälligt filtrera skadlig trafik i internetaccesstjänster.

2. Teleföretaget ska regelbundet kontrollera om de filtreringsåtgärder som används är lämpliga med tanke på deras ändamål, samt se till att filtreringsreglerna är uppdaterade.

3. Teleföretaget ska upprätthålla uppdaterad dokumentation om använda filtreringsåtgärder.

23 Bortkoppling av internetaccesstjänster

1. Teleföretag ska koppla bort ett kundabonnemang från det allmänna kommunikationsnätet om kommunikationstjänstens informationssäkerhet väsentligen äventyras av orsaker som beror på utgående eller inkommande trafik, och om det inte är möjligt att sörja för kommunikationstjänstens informationssäkerhet genom de åtgärder som avses i 22 punkten i denna föreskrift eller med andra lindrigare åtgärder än bortkoppling av kundabonnemanget.

2. Bortkopplingen och återkopplingen ska göras enligt de processer och instruktioner som teleföretaget i förväg har specificerat. I samband med åtgärderna kan speciella förhållanden som beror på abonnemangstyp och informationssäkerhetshotets allvar beaktas.

Kapitel 5 Särskilda krav på tjänster för text- och multimediemeddelanden

24 Filtrering av text- och multimediemeddelandetrafik

1. Teleföretag ska ha behövliga system och tillvägagångssätt att tillfälligt filtrera skadlig trafik i tjänster för text- och multimediemeddelanden.

2. Teleföretag som erbjuder tjänster för text- och multimediemeddelanden ska

   1) märka ut eller filtrera sådan inkommande meddelandetrafik som identifierats som skadlig, om inget annat separat har överenskommits med kunden, och

   2) filtrera sådan utgående meddelandetrafik som identifierats som skadlig.

3. Vad som föreskrivs ovan i första och andra punkten tillämpas inte på tjänster för multimediemeddelanden om företaget för övrigt upptäcker störningar som äventyrar informationssäkerheten och har förmåga att reagera på dem snabbt.

4. Teleföretaget ska regelbundet kontrollera om de tillämpliga filtreringsåtgärderna är lämpliga med tanke på deras ändamål, samt se till att filtreringsreglerna är uppdaterade.

Kapitel 6 Särskilda krav för e-posttjänster

25 Kontaktuppgifter för e-posttjänster och administrering av adressresurser

1. Teleföretag som tillhandahåller e-posttjänster ska se till att företaget har postmaster- och abuse-e-postadresser eller andra abuse-kontaktuppgifter för de domännamn som används för tillhandahållande av e-posttjänster. Meddelanden som kommer till dessa adresser ska kontrolleras regelbundet.

2. Teleföretag som tillhandahåller e-posttjänster får överlåta en e-postadress, som blir ledig, till en annan kund först då sex månader har gått efter det att e-postadressen blev ledig.

26 Särskild skyldighet att filtrera e-posttjänster

1. Teleföretag som tillhandhåller e-posttjänster ska ha till sitt förfogande aktuella och tillförlitliga mekanismer för att identifiera och hantera skadlig e-posttrafik.

2. Teleföretag som tillhandahåller e-posttjänster ska:

   1) filtrera sådan inkommande skadlig trafik som äventyrar informationssäkerheten i de system som används för att producera e-posttjänsten,

   2) märka ut eller filtrera sådan inkommande e-posttrafik som identifierats som skadlig, om inget annat särskilt har överenskommits med kunden, och

   3) filtrera sådan utgående e-posttrafik som identifierats som skadlig.

27 Öppna proxyservrar för e-post

Teleföretag som tillhandahåller e-posttjänster ska se till att de e-postsystem som företaget administrerar inte fungerar som öppna proxyservrar.

28 Förbindelse mellan kund och e-postserver

1. Teleföretag som tillhandahåller e-posttjänster ska som primärt alternativ erbjuda kunderna en skyddad förbindelse mellan kunden och e-postlådan samt mellan kunden och e-postservern för utgående trafik. Skyddet ska genomföras så att användaren av tjänsten identifieras och trafiken krypteras. Skyldigheten gäller också andra än webbläsarbaserade e-posttjänster.

2. De webbläsarbaserade e-posttjänsternas kundförbindelser ska vara skyddade.

Kapitel 7 Ikraftträdandebestämmelser

29 Ikraftträdande [och övergångstid]

1. [Denna föreskrift träder i kraft tre månader efter att föreskriften utfärdats.]

2. Denna föreskrift upphäver Kommunikationsverkets föreskrift 67 A/2015 M om televerksamhetens informationssäkerhet som utfärdades 4.3.2015.

Helsingfors den (dag) (månad) 20(år)

Beslutsfattare

Föredragande

Bilaga 1 Tekniska standarder som ska iakttas

3GPP TS 33.116, Security Assurance Specification (SCAS) for the MME network product class

3GPP TS 33.216, Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class

3GPP TS 33.226, Security assurance for IP Multimedia Subsystem (IMS)

3GPP TS 33.250, Security assurance specification for the PGW network product class

3GPP TS 33.326, Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class

3GPP TS 33.511, Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

3GPP TS 33.512, 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)

3GPP TS 33.513, 5G Security Assurance Specification (SCAS); User Plane Function (UPF)

3GPP TS 33.514, 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class

3GPP TS 33.515, 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class

3GPP TS 33.516, 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class

3GPP TS 33.517, 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class

3GPP TS 33.518, 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class

3GPP TS 33.519, 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

3GPP TS 33.520, 5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)

3GPP TS 33.521, 5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)

3GPP TS 33.522, 5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)

3GPP TS 33.523, 5G Security Assurance Specification (SCAS); Split gNB product classes

3GPP TS 33.526, Security Assurance Specification for Management Function (MnF)

3GPP TS 33.527, Security Assurance Specification (SCAS) for 3GPP virtualized network products

3GPP TS 33.528, Security Assurance Specification (SCAS) for Policy Control Function (PCF) 3GPP TS 33.537, Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF)

[Standarderna ovan som är under beredning ska tas upp i denna bilaga om de publiceras inom ramen för föreskriftens tidtabell.]