



Föreskrift

OM HANTERING AV TELEFÖRETAGENS INFORMATIONSSÄKERHET

Meddelad i Helsingfors den 27 augusti 2009

Kommunikationsverket har med stöd av 19 och 20 § i lagen av den 16 juni 2004 om dataskydd vid elektronisk kommunikation (516/2004), sådan den lyder i lag 125/2009, meddelat följande föreskrift:

1 §

Tillämpningsområde

Denna föreskrift tillämpas på nättjänster och kommunikationstjänster som tillhandahålls i allmänna kommunikationsnät.

2 §

Organisering av informationssäkerheten

Ett teleföretag ska ha en skriftligen definierad dokumentation av organisering av informationssäkerheten med uppgift om olika aktörers ansvar och skyldigheter enligt ansvarsområde. Dokumentationen ska granskas vid behov, dock minst en gång om året. Informationssäkerhetsansvar för personer som innehar ledningsuppgifter inom informationssäkerheten ska framgå av deras befattningsbeskrivningar.

3 §

Styrdokument för informationssäkerhet

Ett teleföretag ska ha en skriftligen definierad och av den högsta ledningen godkänd uppfattning om mål och principer för samt om genomförande av informationssäkerhet samt om kontinuerlig utveckling av systemet för hantering av informationssäkerhet. Uppfattningen ska delges hela personalen i teleföretaget.

Teleföretaget ska dessutom skriftligen dokumentera hur följande specialområden beaktas i den mån de lämpar sig för teleföretagets egen televerksamhet:

- 1) administrativ säkerhet
- 2) personalsäkerhet
- 3) maskin- och programvarusäkerhet
- 4) telekommunikationssäkerhet
- 5) datamaterialsäkerhet
- 6) driftssäkerhet
- 7) ingripande i kränkningar och missbruk av informationssäkerheten.

4 §

Riskhantering

Ett teleföretag ska göra upp en plan för bedömning av riskerna.

Teleföretaget ska identifiera de funktioner, uppgifter och system som är viktiga för televerksamheten.

Teleföretaget ska identifiera och bedöma sådana informationssäkerhetsrisker i funktioner, uppgifter och system som är viktiga för televerksamheten.

Teleföretaget ska ha ett förfarande för att acceptera de betydande risker på vilka inte inriktas några hanteringsåtgärder på basis av evalueringen av riskerna.

Riskhanteringen ska vara systematisk, regelbunden och dokumenterad.

5 §

Informationssäkerhetsåtgärder

Ett teleföretag ska på basis av riskanalysens resultat göra upp en plan som definierar åtgärder, ansvar och tidsscheman för hantering av identifierade risker. Teleföretaget ska regelbundet följa upp hur åtgärderna lämpar sig för användningsändamålet.

Teleföretaget ska definiera detaljerade och tillräckliga anvisningar för enskilda rutiner som är väsentliga för informationssäkerheten. Teleföretaget ska se till att personalen utbildas för att arbeta enligt givna anvisningar.

Teleföretaget ska använda ett system för klassificering av datamaterial som är viktigt för televerksamheten.

Teleföretaget ska se till att händelser som är väsentliga för informationssäkerheten upptäcks. Teleföretaget ska ingripa i upptäckta problem.

6 §

Uppföljning av hanteringen av informationssäkerheten

Genomförandet av skyldigheterna i föreskriften ska granskas regelbundet och alltid vid behov.

7 §

Ikraftträdande och övergångsbestämmelser

Denna föreskrift träder i kraft den 1 september 2009.

Föreskriften är i kraft tills vidare. Genom föreskriften upphävs Kommunikationsverkets föreskrift 47 B/2004 M av den 27 augusti 2004 om informationssäkerhet hos teleföretag.

8 §

Erhållande av upplysningar och publicering

Föreskriften har publicerats i Kommunikationsverkets föreskriftssamling och kan erhållas vid Kommunikationsverkets kundtjänst:

Besöksadress	Östersjögatan 3 A, HELSINGFORS
Postadress	PB 313, 00181 HELSINGFORS
Telefon	09 6966 500
från utlandet	+358 9 6966 500
Telefax	09 6966 410
från utlandet	+358 9 6966 410
Webbplats	http://www.ficora.fi/
FO-nummer	0709019-2

Helsingfors den 27 augusti 2009

Generaldirektör Rauni Hagman

Direktör Timo Lehtimäki