

## **Elektronisko sakaru komersantu Rīcības plāna sagatavošana.**

Pamatojoties uz Ministru kabineta noteikumiem Nr.327 [„Noteikumi par elektronisko sakaru komersantu rīcības plānā ietveramo informāciju, šā plāna izpildes kontroli un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam”](#)

Komentāri:

- Rīcības plānu izstrādā sešu mēnešu laikā pēc šo noteikumu stāšanās spēkā. (MK Noteikumi Nr. 327 punkts 5).
- Ja rīcības plānā iekļautā informācija tiek mainīta, rīcības plānu aktualizē. (MK Noteikumi Nr. 327 punkts 6).
- Rīcības plāna kopiju mēneša laikā pēc tā apstiprināšanas vai aktualizēšanas nosūta IT drošības incidentu novēršanas institūcijai. Nosūtīt rīcības plāna kopiju, elektronisko sakaru komersants norāda, vai tajā iekļautā informācija ir uzskatāma par ierobežotas pieejamības informāciju. (MK Noteikumi Nr. 327 punkts 7). Rīcības plānu var nosūtīt pa pastu uz adresi Informācijas tehnoloģiju drošības incidentu novēršanas institūcijai Raiņa bulvāris 29, Rīga, LV1459, Latvija vai uz elektronisko pastu [kontakti@cert.lv](mailto:kontakti@cert.lv).

### **RĪCĪBAS PLĀNA SATURA RĀDĪTĀJS**

1. Vispārīgas ziņas par komersantu
  - Nosaukums
  - Reģistrācijas numurs
  - Juridiskā adrese
  - Tālrunis, faksa numurs
  - Elektroniskā pasta adrese

Komentāri: Atsauce (MK Noteikumi Nr. 327 punkts 2.1).

2. Persona vai struktūrvienība, kas nodrošina drošības pasākumu īstenošanu
  - Struktūrvienība
  - Persona
  - Tālrunis, faksa numurs
  - Elektroniskais pasts
  - Adrese
  - Darba režīms

Komentāri: Atsauce (MK Noteikumi Nr. 327 punkts 2.2).

Norādot struktūrvienību, lūgums norādīt arī atbildīgo personu, un personu, kura to aizvietos prombūtnes laikā. Ja elektronisko sakaru komersantam ir filiāles vairākos reģionos, informācija jāiesniedz par katru reģionu. Adresi nepieciešams norādīt, ja tā nesakrīt ar komersanta juridisko adresi. Darba režīms – reālais struktūrvienības vai atbildīgās personas darba laiks. Piemēram, darba režīms darba dienās darba laikā (8:00 – 17:00) vai (24x7).

### 3. Elektroniskā sakaru tīkla uzbūve

- Apraksts
  - Ģeogrāfiskā izplatība
  - Centrālie mezgli
    - Pamattīkls
    - Datu centrs
  - Izmantotās datu pārraides tehnoloģijas
    - Optiskā šķiedra
    - Radio inki
    - Kabeļi /DSL
    - Koaksiālie kabeļi (TV infrastruktūra)
    - Cita
- Shēma grafiskā vai tabulārā veidā

Komentāri: Atsauce (MK Noteikumi Nr. 327 punkts 2.3). Elektroniskā sakaru tīkla shēma var būt gan grafiskā, gan tabulārā veidā un tai ir jārada priekšstats par komersanta elektronisko sakaru tīklu.

### 4. Elektroniskā sakaru tīkla risku analīze

- Būtiskākie apdraudējumi
- Risku novērtēšana
- Pasākumi risku ierobežošanai

Komentāri: Atsauce (MK Noteikumi Nr. 327 punkts 2.4).

Risku analīzes piemērs izdomātai/virtuālai iestādei pieejams CERT.LV tīmekļa vietnē (<http://www.cert.lv/section/show/80>)

5. Reaģēšanas kārtība uz drošības incidentiem

- Kārtība kā tiek apstrādātas klientu sūdzības
- Kārtībā kā Elektronisko sakaru komersants sadarbojas ar CERT.LV
  - Paziņošanas kārtība CERT.LV par notikušu incidentu
  - No CERT.LV saņemta ziņojuma par incidentu apstrādes kārtība

Komentāri: Atsauce (MK Noteikumi Nr. 327 punkts 2.5).

CERT.LV incidentu kategorijas, prioritātes un reaģēšanas laiks pieejams CERT.LV tīmekļa vietnē (<http://www.cert.lv/section/show/90> )

6. Elektroniskā sakaru tīkla darbības atjaunošanas plāns

- Kārtība, kā tiek atjaunota pakalpojumu sniegšana.
  - Atbildīgās personas rīcības kārtība
  - Tehniķu rīcības kārtība

Komentāri: Atsauce (MK Noteikumi Nr. 327 punkts 2.5).