Jautājumi un atbildes par Ministru kabineta 2015. gada 28. jūlija noteikumu Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām un to piemērošanu" (turpmāk tekstā - Ministru kabineta noteikumi) piemērošanu.

Atbildēm ir rekomendējošs raksturs un tās neatceļ normatīvajos aktos noteiktās prasības. CERT.LV neuzņemas atbildību par jebkādiem tiešiem, netiešiem, saistītiem, izrietošiem vai īpašiem zaudējumiem, kuri radušies vai var rasties saistībā ar šo atbilžu izmantošanu.

-Vai uz mums attiecas Ministru kabineta noteikumu prasības?

Ministru kabineta noteikumu prasības attiecas uz visām valsts un pašvaldību institūciju pārziņā vai turējumā esošām informācijas un komunikācijas tehnoloģiju sistēmām, izņemot informācijas un komunikācijas tehnoloģiju sistēmas (turpmāk - Sistēmas), kurās tiek veikta valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu institūciju klasificētās informācijas vai informācijas dienesta vajadzībām apstrāde vai uzglabāšana, kā arī uz kritiskās infrastruktūras informācijas sistēmām.

- Vai nosacījumi par Sistēmas uzlabošanu attiecas, ja to dara paši?

Ministru kabineta noteikumu 21. un 22. punkta prasības iekļaut iepirkuma specifikācijā drošības prasības attiecas tikai uz gadījumiem, kad tiek veikts iepirkums par jaunas Sistēmas izstrādi vai esošās uzlabojumiem.

- Vai MK noteikumos minētās prasības jāuzskata par kontrolēm?

Ministru kabineta noteikumu 15.un 24.punktā ir uzskaitītas prasības, kas iekļaujamas institūcijas drošības dokumentācijā un pret ko iespējams novērtēt dokumentācijas atbilstību.

- Kas veic informācijas klasificēšanu institūcijā un kas nosaka sistēmas kategoriju?

Informācijas klasificēšanu institūcijā veic saskaņā ar Informācijas atklātības likumu, savukārt, Sistēmas kategoriju nosaka atbildīgā persona saskaņā ar Ministru kabineta noteikumu 7.punktā noteikto metodiku.

- Vai rīcība incidenta gadījumā ir jāliek atjaunošanas plānā?

Sistēmas atjaunošanas plānā būtu vēlams iestrādāt kritērijus, kādu incidentu gadījumos tiek piemērots atjaunošanas plāns (piemēram, laiks, cik ilgi sistēma nav pieejama, zudušo datu apjoms).

- Ja tiek izmantots Valsts informācijas sistēmu savietotājs, kādas ir pieejamības prasības?

Prasības Valsts informācijas sistēmu savietotājam (http://www.vraa.gov.lv/lv/epakalpojumi/viss/) tiek noteiktas līgumā ar Valsts reģionālās attīstības aģentūru .

- Kas ir sensitīvi personas dati?

Saskaņā ar Fizisko personu datu aizsardzības likumu sensitīvi personas dati ir personas dati, kas norāda personas rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi. Datu valsts inspekcija ir sagatavojusi rekomendācijas par personas datu apstrādi un aizsardzību darba vietās http://www.dvi.gov.lv/lv/latvijas-normativie-akti/metodiskie-noradijumi/

- Vai ar Windows autentifikāciju pietiek, lai pēc tam lietotu Sistēmas?

Jā, ir pietiekami izmantot Windows autentifikāciju. Single Sign-On noteiktos gadījumos ir pieļaujams izmantot.

- Ieteicamie Sistēmas resursu valdītāji?

Ieteicams par tehnisko resursu valdītāju noteikt darbinieku, kas pārzina Sistēmas tehniskos resursus un spēj nodrošināt to veiksmīgu darbību. Informācijas resursu valdītājs ir darbinieks, kas atbild par attiecīgo iestādes funkciju vai pakalpojumu, ko nodrošina sistēma.

- Vai noteikumu prasības attiecas arī tad, ja pakalpojumu sniedz viena valsts iestāde citai valsts iestādei?

Ministru kabineta noteikumi nosaka prasības, kas jāiekļauj ārpakalpojumu līgumos, neatkarīgi no tā, kas ir ārpakalpojuma sniedzējs.