SABIEDRĪBAS AR IEROBEŽOTU ATBILDĪBU "ELEKTRONISKIE SAKARI" INFORMĀCIJAS UN KOMUNIKĀCIJU TEHNOLOĢIJU KIBERDROŠĪBAS PĀRVALDĪBAS NODROŠINĀJUMA PAMATA NOSTĀDNES

Dokumenta mērķis

Sabiedrības ar ierobežotu atbildību "Elektroniskie sakari" (turpmāk – Sabiedrība) Informācijas un komunikāciju tehnoloģiju kiberdrošības pārvaldības nodrošinājuma pamata nostādņu mērķis ir noteikt pamata nosacījumus un pieejas, kuras Sabiedrība īsteno kiberdrošības pārvaldības un pārraudzības pamatnostādņu izpildei attiecībā uz Sabiedrības pārziņā esošajiem informācijas un komunikāciju tehnoloģiju risinājumiem un elektroniska formāta informācijas resursiem. Sabiedrība Informācijas un komunikāciju tehnoloģu kiberdrošības pārvaldību īsteno saskaņā ar Sabiedrībā ieviestu informācijas drošības vadības sistēmu, kura ir sertificēta atbilstoši standarta ISO 27001 nosacījumiem.

Informācijas un komunikāciju tehnoloģiju drošības pārvaldības pamata principi

1. Sabiedrība, veicot savu biznesa darbību, tajā piemēro un ietver Informācijas un komunikāciju tehnoloģiju kiberdrošības pārvaldības principus , kuri ir vērsti uz Sabiedrības rīcībā esošās elektroniska formāta informācijas konfidencialitātes nodrošināšanu un nepārtrauktu Sabiedrības funkciju izpildes īstenošanu, kas aptver visus Sabiedrības rīcībā esošos informācijas sistēmu un tehnoloģiskos risinājumus.

2. Sabiedrība, īstenojot Informācijas un komunikāciju tehnoloģiju kiberdrošības pārvaldību, ievēro visus tai saistošos ārējos normatīvos aktus attiecīgajā jomā.

3. Sabiedrība savu Informācijas un komunikāciju tehnoloģiju kiberdrošības pārvaldības vidi veido, ievērojot šādus pamata principus:

   3.1. Informācijas un komunikāciju tehnoloģiju kiberdrošības pārvaldība tiek organizēta un kontrolēta piemērojot strukturētu atbildības sadalījumu, paredzot izdalītas atbildīgās personas noteikšanu par Informācijas un komunikāciju tehnoloģiju kiberdrošības jomu Sabiedrībā.

   3.2. Informācijas sistēmu un tehnoloģisko risinājumu izveide, izstrāde, testēšana un ieviešana produkcijas vidē tiek veikta kontrolētā veidā, pārvaldot katru no attiecīgajiem posmiem un nodrošinot, ka tiek ieviesta tikai tāda informācijas sistēma, tehnoloģiskais risinājums vai to izmaiņas, kas ir atbilstoši notestētas un pārbaudītas pret iespējamajiem kiberdrošības apdraudējumiem vai nepilnībām.

   3.3. Informācijas sistēmu resursi tiek izvietoti uz tehniskajiem resursiem, kuri atrodas atbilstošās telpās, kas ir aizsargātas ar pienācīgiem fiziskās un loģiskās aizsardzības pasākumiem.

   3.4. Piesaistot ārējos pakalpojumu sniedzējus Informācijas un komunikāciju tehnoloģiju resursu garantijas apkalpošanai, uzturēšanai un attīstības pasākumu veikšanai, tiek nodrošināta attiecīgo ārējo pakalpojumu sniedzēju atbilstības novērtēšana attiecībā pret spēkā esošajos ārējos un iekšējos normatīvajos aktos noteikto prasību izpildi kiberdrošības pārvaldības jomā.

   3.5. Visas izmaiņas Informācijas sistēmās un tehniskajos risinājums tiek veiktas kontrolētā veidā, kas ļauj atsekot to nepieciešamību, izstrādes pasākumu veikšanas secību, un to izmaiņu ieviešanas ietvaros tiek piemēroti nepieciešamie kiberdrošības pasākumi.

   3.6. Pārstājot izmantot Informācijas sistēmu vai pēc jaunas Informācijas sistēmas ieviešanas, kura funkcionāli aizvieto kādu esošo Informācijas sistēmu, tiek nodrošināta novecojušās informācijas sistēmas izvietošana arhīva režīmā, vai tās pilnīga darbības pārtraukšana, īstenojot pasākumus Informācijas dzēšanai.

   3.7. Elektroniskās formas informācijas apmaiņa ārpus Sabiedrības tiek veikta veidā, kas ļauj izsekot Informācijas plūsmas, Informācijas apmaiņai pakļauto datu apjomu un Informācijas apmaiņas subjektu.

   3.8. Elektroniskās formas informācijas izmantošana tiek pārvaldīta veidā, kas ļauj katru veikto darbību izsekot līdz konkrēta lietotāja līmenim, ieviešot nepieciešamās procedūras Tehnisko resursu vadības un kontroles pasākumu īstenošanai.

   3.9. Piekļuve pie Informācijas un komunikāciju tehnoloģiju resursiem tiek piešķirta tikai tādā apjomā, kāds ir nepieciešams konkrētā lietotāja vai trešās puses darba pienākumu izpildei, nodrošinot atbilstošu

autentifikācijas līdzekļu piemērošanu un lietošanu un vienotu lietotāju identifikācijas parametru izmantošanu.

3.10. Informācijas sistēmām tiek veidotas, uzglabātas un pārbaudītas to rezerves kopijas, kas nodrošina Informācijas apjaunošanas iespējas atbilstoši Sabiedrības Informācijas sistēmu darbības nepārtrauktības prasībām.

3.11. Elektroniskas formas informācijas pārvietošana, izmantojot portatīvos datu nesējus, tiek ierobežota līdz iespējami zemākajam līmenim un tiek nodrošināta aizsardzības pasākumu īstenošana portatīvo datu nesēju pārvaldībai.

3.12. Informācijas un komunikāciju tehnoloģiju vidē notiekošās darbības tiek auditētas, nodrošinot auditācijas pierakstu centralizētu uzkrāšanu un apstrādi iespējamo aizdomīgo darbību identificēšanai un izmeklēšanai.

3.13. Tehnisko resursu nomaiņa tiek plānota, organizēta un veikta kontrolētā veidā, paredzot, ka attiecīgās izmaiņas iespējami mazākajā mērā ietekmē Sabiedrības kopējo darbību un neatstāj negatīvu ietekmi uz Sabiedrības darbības nepārtrauktību.

3.14. Sabiedrībā tiek izstrādāta, uzturēta un pārvaldīta procedūra Informācijas drošības incidentu vadībai, kas paredz kompetento struktūrvienību iesaisti, sadarbību un pasākumu veikšanu iespējamās negatīvās ietekmes mazināšanai.

3.15. Sabiedrībā tiek īstenoti regulāri pasākumi darbinieku izglītošanai attiecībā uz Informācijas un komunikāciju tehnoloģiju un Informācijas drošības pārvaldības prasībām, kuras ir definējusi Sabiedrība, lai nodrošinātu izpratnes un zināšanu attīstību par iespējamajiem drošības apdraudējumiem un veicamo rīcību gadījumos, kad darbinieks ir saskāries ar noteiktu apdraudējumu.

3.16. Sabiedrības darbiniekiem un piesaistītajām trešajām pusēm tiek noteiktas konkrētas tiesības, pienākumi un atbildība attiecībā uz pasākumiem, kuri ir veicami Sabiedrības Informācijas un komunikāciju tehnoloģiju kiberdrošības pārvaldības nodrošināšanai.

3.17. Sabiedrībā tiek izstrādāta, uzturēta un pārvaldīta procedūra Informācijas sistēmu lietotāju tiesību pārvaldībai, kas nodrošina pieejas tiesību pieprasījumu atsekojamību un iespēju kontrolēt pieejas tiesību atbilstību konkrēto Sabiedrības darbinieku vai piesaistīto trešo pušu veicamajiem darba pienākumiem.

3.18. Sabiedrībā tiek precīzi definēti pieļaujamie autentifikācijas mehānismi piekļuvei pie Informācijas sistēmām, nosakot to darbības principus un pārvaldībai veicamos pasākumus.

3.19. Sabiedrības rīcībā esošās portatīvās iekārtas tiek pārvaldītas izmantojot Sabiedrībai pieejamus aizsardzības pasākumus un tiek nodrošināta to izmantošana tikai darba pienākumu izpildes vajadzībām.

3.20. Sabiedrībā tiek nodrošināta attālinātā darba kontroles pasākumu veikšana un tehnisko risinājumu ieviešana, kas nodrošina drošu attālināto darbu.

3.21. Sabiedrībā tiek izstrādāta, uzturēta un pārvaldīta procedūra Informācijas un komunikāciju tehnoloģiju lietotāju atbalsta nodrošināšanai, paredzot pieteikumu apstrādes atsekojamību un izpildes gaitas informācijas apkopošanu.

3.22. Sabiedrības veikti pasākumi informācijas sistēmu izstrādei, tiek īstenoti piemērojot iespējami augstākos kiberdrošības standartus un labas prakses piemērus.

3.23. Sabiedrība īsteno regulāras iekšējā un ārējā audita aktivitātes savas informācijas un komunikāciju tehnoloģiju kiberdrošības atbilstības novērtēšanai un iespējamo tālāko veicamo pilnveides pasākumu īstenošanai.

3.24. Sabiedrība veic pasākumus savas ieviestās informācijas drošības vadības sistēmas uzturēšanai, regulārai pārskatīšanai un pilnveidošanai.