

IT drošības politikas pamatnostādnes

Informācijas tehnoloģiju (IT) drošības politikas pamatnostādņu (turpmāk – pamatnostādnes) mērķi ir paust koncerna “Latvijas Finieris” uzņēmuma nostāju un atbalstu IT drošības nodrošināšanai atbilstoši koncerna vajadzībām, spēkā esošajam tiesiskajam regulējumam, kā arī nodrošināt koncerna uzņēmumu rīcībā esošo informācijas un tehnoloģiju resursu aizsardzību pret dažāda veida draudiem tā, lai draudu īstenošanas iespējamība būtu pieņemamā līmenī.

Koncerna “Latvijas Finieris” IT drošības politikas pamatnostādnes ir:

- “Latvijas Finieris” nodrošina tādu IT un komunikāciju vidi, lai tā rīcībā esošie informācijas un tehnoloģiskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības riskiem, vienlaikus nodrošinot uzņēmuma nepārtrauktu un kvalitatīvu darbu.
- Drošības prasību ieviešana un risku ierobežošanas nodrošināšana ir samērīga ar pieejamo resursu apjomu un iespējamajiem zaudējumiem, kas varētu rasties šo risku iestāšanās gadījumā.
- “Latvijas Finieris” tiek sekmēta katra darbinieka izpratne par pienākumiem risku un darbības nepārtrauktības pārvaldīšanā un informācijas un tehnoloģisko resursu aizsardzības nodrošināšanā, nodrošinot regulāru darbinieku izglītošanu.

Pamatnostādnes tiek īstenotas saskaņā ar “Latvijas Finiera” vērtībām un mērķiem, kā arī saskaņā ar spēkā esošajiem normatīvajiem aktiem.

Pamatnostādnes veido pamatu informācijas drošības pārvaldībai koncerna uzņēmumos, procedūru, instrukciju un citu nepieciešamo iekšējo normatīvo aktu izstrādei un ieviešanai.

Pamatnostādnes attiecas uz koncerna “Latvijas Finieris” uzņēmumu pārvaldībā esošajiem informācijas un tehniskajiem resursiem un ir saistoša visiem informācijas sistēmu lietotājiem, kuru ir tiesīgi izmantot AS “Latvijas Finieris” pārvaldībā esošos informācijas un tehniskos resursus, kā arī tiem ārpalpojumu sniedzējiem, kuri AS “Latvijas Finieris” sniedz ar informācijas tehnoloģijām saistītus pakalpojumus.

AS “Latvijas Finieris” IT drošības pārvaldības dokumentus aktualizē ne retāk kā reizi trīs gados, kā arī tajos gadījumos, kad veiktās izmaiņas sistēmās vai informācijas tehnoloģiju infrastruktūrā var ietekmēt informācijas sistēmu drošību, ja mainījušies vai ir atklāti jauni sistēmas apdraudējumi vai, ja pieaug sistēmas drošības incidentu skaits vai noticis nozīmīgs sistēmas drošības incidents.