Sabiedrība ar ierobežotu atbildību

RĒZEKNES NAMSAIMNIEKS

Atbrīvošanas aleja 106, Rēzekne, LV – 4601, Reģ. Nr. 40003215461
Tālrunis 64639000, fakss 64605967, e-pasts: rezeknes.namsaimnieks@apollo.lv

Rēzeknē

SIA "RĒZEKNES NAMSAIMNIEKS"
INFORMĀCIJAS SISTĒMAS DROŠĪBAS POLITIKA

1. Vispārīgie noteikumi

1. Informācijas sistēmas drošības politika (turpmāk – Politika) nosaka pamatprincipus, kādos SIA "Rēzeknes Namsaimnieks" (turpmāk – Sabiedrība) nodrošina informācijas, Informācijas sistēmu un saistīto tehnoloģisko resursu drošību, pieejamību, integritāti un konfidencialitāti saskaņā ar spēkā esošajiem normatīvajiem aktiem.
2. Sabiedrības pienākums ir nodrošināt, lai tās rīcībā esošā informācija tiktu apstrādāta, glabāta un pārvaldīta droši un pārbaudāmi, sniedzot tās darbiniekiem un Lietotājiem skaidri noteiktas prasības informācijas sistēmas iekārtu un resursu izmantošanā, un nodrošināt Informācijas sistēmu aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem.
3. Politika ir izstrādāta kā pamatdokuments, kas nosaka galvenos drošības pamatnosacījumus informācijas tehnoloģiju videi un definē kārtību informācijas un tehnoloģisko resursu aizsardzības nodrošināšanai.
4. Politika ir izstrādāta saskaņā ar Informācijas tehnoloģiju drošības likumu, Valsts informācijas sistēmu likumu, Fizisko personu datu aizsardzības likumu, 2015. gada 28. jūlija Ministru kabineta noteikumu Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8. punktu.
5. Politika attiecas uz Sabiedrības pārvaldībā esošiem informācijas un tehniskajiem resursiem, un ir saistoša visiem Sabiedrības darbiniekiem, kuri ir tiesīgi izmantot Sabiedrības pārvaldībā esošos informācijas un tehniskos resursus, kā arī tiem ārpakalpojumu sniedzējiem, kuri Sabiedrībai sniedz ar informācijas tehnoloģijām saistītus pakalpojumus.
6. Izstrādājot vai koriģējot iekšējos normatīvos aktus informācijas tehnoloģiju jomā, ir jāievēro Politikā noteiktās normas un principi.
7. Sabiedrība informācijas drošības pārvaldības dokumentus pārskata vismaz reizi gadā un aktualizē, ja tiek konstatēta atbilstoša nepieciešamība, kā arī gadījumos: 7.1. ja izmaiņas Informācijas sistēmās var ietekmēt to drošību; 7.2. ja mainījušies vai ir atklāti jauni Informācijas sistēmu drošības apdraudējumi; 7.3. ja noticis nozīmīgs Informācijas sistēmu drošības incidents; 7.4. ja izdarīti grozījumi spēkā esošajos normatīvajos aktos, kas regulē informācijas drošību vai Informācijas sistēmu darbību.
8. Politiku izstrādā, aktualizē un pārskata Sabiedrības Informācijas sistēmu drošības pārvaldnieks un apstiprina Sabiedrības padome.
9. Politikā lietoto terminu skaidrojums:
   9.1. **Informācijas sistēma** - datu ievadīšanas, uzglabāšanas, apstrādes un pārraidīšanas sistēma, kurā glabātajiem datiem vai informācijai ir paredzēta Sistēmas lietotāju pieeja vai kas lietotājiem sniedz informācijas pakalpojumus;

9.2. **Informācijas resurss** – Sabiedrības rīcībā esošas (radītas vai saņemtas) ziņas, fakti vai ziņu un faktu kopums jebkurā tehniski iespējamā fiksēšanas, uzglabāšanas vai nodošanas veidā;
9.3. **Tehniskais resurss** – fiziskie serveri un tajos uzstādāmā serveru programmatūra, datu krātuves, gala lietotāju datori, datortīklu aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai;
9.4. **Tīkla resurss** – Programmiskais, tehniskais, informacionālais un organizatoriskais datoru tīkla nodrošinājums, kas paredzēts lietotāju uzdevumu risināšanai;
9.5. **Lietotājs** – persona, kurai ir tiesības piekļūt un veikt darbības noteiktā Informācijas sistēmā vai Tīkla resursā;
9.6. **Pārzinis** – persona, kuras kompetencē atrodas informācijas, Informācijas sistēmas vai Tehniskā resursa pārvaldība;
9.7. **Informācijas sistēmu drošības pārvaldnieks** – Sabiedrības darbinieks vai ārpakalpojuma sniedzējs, kurš nodrošina informācijas sistēmu drošības pārvaldības organizēšanu un izpildes kontroli;
9.8. **Zaudējums** – jebkāds Sabiedrības mantas samazinājums, zudums vai bojājums, peļņas atrāvums, papildu izdevums un citas mantiski novērtējamas tiesību aizskāruma sekas;
9.9. **Drošības pārvaldība** – nepieciešamo resursu un veikto/veicamo pasākumu kopums, lai nodrošinātu informācijas tehnoloģiju drošības pasākumu īstenošanu Sabiedrībā atbilstoši Politikā noteiktajam.

2. Informācijas drošības politikas mērķis un pamatnostādnes

10. Sabiedrība izvirza šādus stratēģiskos mērķus informācijas drošības jomā:
10.1. Sabiedrības pakalpojumu nepārtrauktības nodrošināšana;
10.2. fizisko personu datu aizsardzības prasību nodrošināšana;
10.3. ārējo normatīvo aktu prasībām un līgumsaistībām atbilstošu informācijas aizsardzības pasākumu nodrošināšana;
10.4. Sabiedrības reputācijas aizsargāšana no nesankcionētas informācijas izpaušanas radītām sekām;
10.5. efektīvas informācijas drošības pārvaldības sistēmas izveidošana;
10.6. preventīvo pasākumu nodrošināšana pret izplatītākajiem informācijas apdraudējuma veidiem;
10.7. Informācijas sistēmu, tehnisko un tehnoloģisko risinājumu ieviešana un uzlabošana atbilstoši informācijas drošības industrijas labākās prakses standartiem;
10.8. regulāras sadarbības uzturēšana ar kompetentajām iestādēm informācijas drošības jomā.
11. Visa Sabiedrības informācija uzskatāma par vērtību, kas aizsargājama pret jebkāda veida neautorizētu apstrādi, tajā skaitā neautorizētu piekļūšanu, lietošanu, modificēšanu, dzēšanu, noplūdi u.c.
12. Risku ierobežošanas un darbības nepārtrauktības nodrošināšanas darbību izmaksas nedrīkst pārsniegt iespējamos Zaudējumus, kas varētu rasties šo risku iestāšanās gadījumā.
13. Sabiedrībā tiek sekmēta katra Informācijas resursa Lietotāja izpratne par pienākumiem risku darbības nepārtrauktības pārvaldīšanā un informācijas aizsardzības nodrošināšanā, veicot ikgadēju izglītošanu.

3. Informācijas drošības politikas īstenošanas pamatprincipi

14. Sabiedrībā ir noteikts un pastāvīgi tiek pilnveidots dokumentu un pasākumu kopums, kuru īstenošana nodrošina Politikas mērķu sasniegšanu.

15. Informācijas drošības pasākumu organizēšanu un iekšējo normatīvu aktu izstrādi, papildināšanu un atjaunošanu Sabiedrība veic saskaņā ar spēkā esošajiem normatīvajiem aktiem un standartiem.
16. Visiem informācijas drošības nodrošināšanas un pārvaldības procesiem Sabiedrībā jābūt vadāmiem, tas ir, jābūt spējai uzraudzīt procesus un komponentus, savlaicīgi atklāt informācijas drošības pārkāpumus un veikt atbilstošus pasākumus.
17. Sabiedrība cenšas identificēt, ņemt vērā un ātri reaģēt uz faktiski notiekošajiem un iespējamiem informācijas drošības pārkāpumiem, kā arī veikt incidentu dokumentēšanu un uzskaitīšanu.
18. Sabiedrība nepārtraukti īsteno pasākumus informācijas drošības risku novērtēšanai un pārvaldīšanai, kā arī informācijas drošības līmeņa paaugstināšanai.
19. Informācijas sistēmu drošības procesu īstenošanas pasākumi Sabiedrībā, kas nav konkretizēti Politikā un attiecas uz visiem Sabiedrības darbiniekiem, ir nosakāmi ar valdes locekļa lēmumu.
20. Gadījumos, kad Sabiedrības darbinieks neievēro Politiku un citas Informāciju sistēmu reglamentējošās prasības, valdes loceklis ir tiesīgs ierosināt darbinieka disciplinārās sodīšanas procesu saskaņā ar spēkā esošajiem normatīvajiem aktiem.

4. Drošības organizācija

21. Valdes loceklis kontrolē Politikas īstenošanu Sabiedrībā un nodrošina resursu piešķiršanu informācijas tehnoloģiju Drošības pārvaldības pilnvērtīgai funkcionēšanai.
22. **V**aldes locekļa nozīmētā atbildīgā persona par Sabiedrības tehniskajiem resursiem nodrošina Politikas īstenošanu Sabiedrībā.
23. Informācijas tehnoloģiju drošības pārvaldības īstenošanai Sabiedrības valdes loceklis nosaka Informācijas sistēmu drošības pārvaldnieku.
24. Informācijas sistēmu drošības pārvaldnieks ir atbildīgs par konkrētu informācijas tehnoloģiju drošības pasākumu īstenošanu, koordinēšanu un izpildes uzraudzību, informācijas tehnoloģiju drošības incidentu analīzi un izmeklēšanu. Informācijas sistēmu drošības pārvaldnieks apkopo izanalizēto incidentu rezultātus un, ja nepieciešams, ziņo Sabiedrības Informācijas tehnoloģiju departamenta vadītājam turpmākas disciplinārlietas ierosināšanas izvērtēšanai.
25. Sabiedrība informācijas drošības pārvaldību balsta uz normatīvo aktu prasībām, kas precīzi un nepārprotami definē Informācijas sistēmas Lietotāja, Informācijas sistēmas Pārziņa, Informācijas sistēmas resursa Pārziņa, Informācijas sistēmas Tehniskā resursa pārziņa, ārpakalpojuma sniedzēja un Informācijas sistēmu drošības pārvaldnieka pienākumus un tiesības, darbojoties ar Sabiedrības resursiem.
26. Informācijas sistēmas Lietotāja pienākums ir ievērot Politikas un citu iekšējo normatīvo aktu noteikumus, kā arī rūpēties par informācijas resursu konfidencialitātes, pieejamības un integritātes saglabāšanu Sabiedrībā.
27. Informācijas sistēmas Lietotājs ir atbildīgs par visām darbībām, kas veiktas ar viņam piešķirto lietotājvārdu. Informācijas resursa Lietotāja pienākums ir informēt savu tiešo vadītāju vai kontaktpersonu (ja Informācijas resursa Lietotājs nav Sabiedrības darbinieks) un Informācijas sistēmu drošības pārvaldnieku par visiem informācijas tehnoloģiju drošības incidentiem, aizdomīgiem notikumiem vai Informācijas drošības politikas pārkāpumiem.
28. Darbinieki, kuru darba pienākums ir nodrošināt Informācijas sistēmu vai Tehnisko resursu darbību, ir atbildīgi par regulāru uzraudzību un preventīvu pasākumu veikšanu, lai nodrošinātu ilgtspējīgu, Politikas un normatīvo aktu prasībām atbilstošu Informācijas sistēmu darbību.
29. Līgumu sagatavotāji ir atbildīgi par Politikas ievērošanu, slēdzot līgumus ar sadarbības partneriem, piegādātājiem, klientiem, uzņēmējiem, konsultantiem u.c. un informācijas neizpaušanas prasību ietveršanu slēdzamajos līgumos. Līgumos jānosaka Informācijas sistēmu

resursu drošības prasības un jāparedz Sabiedrības tiesības izbeigt līgumattiecības līgumos noteikto drošības prasību neievērošanas gadījumos.

2020.gada 01.janvārī

Valdes loceklis P. Dzalbe

PERSONAS DATU DROŠĪBAS INCIDENTU REĢISTRS
Nomenklatūras Nr. 5.6.

Datums	Numurs	Incidenta īss apraksts	Iesaistītie darbinieki	Iesaistītās trešās personas	Pielikumi