SIA „JAUNROTA”
INFORMĀCIJAS SISTĒMAS DROŠĪBAS POLITIKA UN LIETOŠANAS NOTEIKUMI

I.VISPĀRĪGIE JAUTĀJUMI

1. Informācijas sistēmas drošības politika nosaka politiku, kādā Sabiedrība ar ierobežotu atbildību „JAUNROTA” (turpmāk – Sabiedrība) nodrošina Sabiedrības izmantotās informācijas sistēmas aizsardzību pret ārējiem un iekšējiem riskiem, nosaka darbinieku pienākumus un prasības Sabiedrības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta Sabiedrības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Informācijas sistēmas drošības politika attiecas uz Sabiedrības Informācijas sistēmas lietotājiem, kuriem ir pieeja kādai(ām) no informāciju sistēmām (piemēram, grāmatvedībā - Zalktis, videonovērošanas sistēma).

3. Politikā lietotie termini:

3.1. Informācijas sistēma – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta Sabiedrības funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

3.2. Sabiedrība ar ierobežotu atbildību „JAUNROTA” – kapitālsabiedrība, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.

3.3. Sistēmas drošības pārvaldnieks ir valdes priekšsēdētājs, kurš atbild par Sabiedrības informācijas sistēmas drošības pasākumu izstrādi, ieviešanu un uzturēšanu, kā arī rīkojas ar informācijas resursiem, un kurš rīkojas bez īpaša pilnvarojuma veikt šīs darbības.

3.4. Informācijas sistēmas lietotājs – darbinieks, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

4. Informācijas sistēmas drošības politika ir izstrādāta saskaņā ar spēkā esošajiem tiesību aktiem, tai skaitā Vispārējo datu aizsardzības regulu.

II. INFORMĀCIJAS SISTĒMAS DROŠĪBAS POLITIKAS MĒRĶI UN PAMATNOSTĀDNES

5. Sabiedrības pienākums ir nodrošināt, lai to 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 nodrošinot Informācijas sistēmas aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem.

6. Informācijas sistēmas drošības politika attiecas uz visiem Sabiedrības Informācijas sistēmas lietotājiem, kuri veic darbības ar informācijas resursiem (piemēram, informācijas sistēmām, informāciju, kas tiek saņemta, apstrādāta, ievadīta, pārsūtīta vai uzglabāta) un tehniskajiem resursiem (piemēram, datoru sistēmām, datoru tīkliem).

7. Informācijas sistēmas lietotājs, kas ir nodarbināts Sabiedrībā un ir Sabiedrības darbinieks, atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šajā dokumentā.

8. Informācijas sistēmu lietotāji pirms sistēmu lietošanas uzsākšanas tiek iepazīstināti ar Sabiedrības iekšējiem normatīvajiem aktiem par datu aizsardzību un šo dokumentu.

9. Valdes priekšsēdētājs atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šajā dokumentā.

10. Valdes priekšsēdētājs ir atbildīgs par viņa pakļautībā vai uzraudzībā esošajiem Informācijas sistēmas lietotājiem. Valdes priekšsēdētājs nodrošina, ka personāls, uz kuru šī politika attiecas daļēji vai pilnā apmērā, ir informēts par politikas esamību un pilda savus darba pienākumus atbilstoši politikas nostādnēm.

11. Informācijas sistēmas drošība tiek nodrošināta šādu mērķu realizācijai:

11.1. nodrošinātu informācijas pieejamību;
11.2. nodrošinātu informācijas integritāti;
11.3. nodrošinātu informācijas konfidencialitāti;
11.4. aizsargātu sistēmas informācijas resursus;
11.5. aizsargātu sistēmas tehniskos resursus;
11.6. noteiktu sistēmas drošības apdraudējumu;
11.7. novērtētu sistēmas drošības risku;
11.8. atklātu sistēmas drošības incidentu;
11.9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.

12. Sabiedrībā izmantotās informācijas sistēmas nav iedalītas klasēs, jo Sabiedrība apstrādā publiski pieejamu informāciju un sistēmā glabātās informācijas neatļauta izpaušana vai noplūde nerada risku Sabiedrībai, sistēmā glabāto datu integritātes apdraudējums nerada risku Sabiedrības pamatfunkciju nodrošināšanai.

13. Sabiedrībā netiek izmantotas informācijas sistēmas, kurās tiktu apstrādāti sensitīvi personas dati un kas ir uzskatāmas par paaugstinātam drošības sistēmām.

14. Ar informācijas tehnoloģiju drošības pārvaldību, atbalstu un lietošanu saistītās funkcijas veic valdes priekšsēdētājs.

III. INFORMĀCIJAS SISTĒMAS DROŠĪBAS ORGANIZĀCIJA

15. Informācijas sistēmas drošības organizatoriskās struktūras pamatu veido valdes priekšsēdētājs un Informācijas sistēmas lietotāji.

16. Valdes priekšsēdētājs nodrošina informācijas sistēmas drošības politikas realizāciju, kā arī veic šādas darbības:

16.1. Pēc nepieciešamības pārskata un aktualizē šo dokumentu;
16.2. nodrošina informācijas sistēmās izmantojamās informācijas racionālu un pareizu izmantošanu.
16.3. izskata informācijas sistēmas lietotāju tiesību piešķiršanas un izmaiņu veikšanas pieteikumu autorizāciju.
16.4. nodrošina atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši šīs politikas prasībām.
16.5. nodrošina tehnisko resursu racionālu un pareizu izmantošanu.
16.6. nodrošina tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus.
16.7. nodrošināt informācijas sistēmas atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un informācijas sistēmas funkcionēšana traucēta vai neiespējama.
16.8. nodrošināt atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus.

17. Sabiedrības valdes priekšsēdētājs nodrošina Sabiedrības Informācijas sistēmas lietotāju apmācību informācijas sistēmu drošības jomā, izskaidrojot tiem Informācijas sistēmas drošības politikas pamatprincipus un būtiskākos drošības pasākumus datu drošībai.

IV. TEHNISKO RESURSU FIZISKĀ DROŠĪBA

18. Sabiedrības datorsistēmas un tehnika (t.sk. datortīkli, programmatūra, informācijas sistēmas, datori) tiek aizsargāta ar piemērotu fizisko, tehnisko, organizatorisko un vides kontroļu kopumu.

19. Datori tiek novietoti telpās, kurās pieeja ir tikai atbilstošām personām, nodrošinot fizisko aizsardzību no nepiederošām trešajām personām pret piekļūšanu šiem resursiem. Par datoru fizisko drošību atbild attiecīgais darbinieks.

20. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) darbiniekam ir nekavējoši jāpaziņo Sabiedrības valdes priekšsēdētājam.

21. Valdes priekšsēdētājs veic pasākumus datoru vīrusu darbības novēršanai tehniskajos resursos, izmantojot šim nolūkam paredzētu programmatūru.

.

22. Nepiederošas personas, t.sk. klienti, ārējie pakalpojumu sniedzēji, biroja vai tirdzniecības vietu telpās drīkst uzturēties tikai sabiedrības darbinieku vai vadības klātbūtnē.

23. Datu nesēju (t.sk. CD, DVD, USB Flash, ārējais cietais disks vai tml.) fizisko aizsardzību nodrošina katrs Informācijas sistēmas lietotājs, nodrošinot, ka tie tiek glabāti drošās vietās, lai novērstu jebkādu nepilnvaroto personu piekļuvi.

24. Sabiedrības valdes priekšsēdētājs organizē elektronisko datu nesēju iznīcināšanu un nodrošina šo iznīcināto elektronisko datu nesēju uzskaiti.

V. INFORMĀCIJAS SISTĒMAS LIETOTĀJU ADMINISTRĒŠANAS KĀRTĪBA

25. Sabiedrības valdes priekšsēdētājs ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

26. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Sabiedrības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

27. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Sabiedrības informācijas resursiem personām, kuras nav Sabiedrības darbinieki, notiek tikai atsevišķos gadījumos pēc Sabiedrības valdes priekšsēdētāja lēmuma (piemēram, gadījumā ja ir noslēgts līgums starp Sabiedrību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

28. Piešķirtās lietotāju pieejas tiesības Sabiedrības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

28.1. darbiniekiem, kuri pārtrauc darba (un citu līgumu) tiesiskās attiecības ar Sabiedrību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

28.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar Sabiedrību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

29. Sabiedrības valdes priekšsēdētājam ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (un personas, kuras darbojas uz citu līgumu pamatiem) pienākumiem un specifikai.

VI. INFORMĀCIJAS SISTĒMAS LIETOTĀJU TIESĪBAS, PIENĀKUMI UN ATBILDĪBA

30. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

31. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

32. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Sabiedrības valdes priekšsēdētājs.

33. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu Sabiedrības datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Sabiedrības valdes priekšsēdētājs.

34. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Sabiedrības valdes priekšsēdētāja atļaujas ir aizliegta.

35. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Sabiedrības valdes priekšsēdētājs.

36. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Sabiedrības telpām drīkst iznest tikai ar Sabiedrības valdes priekšsēdētāja RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no Sabiedrības telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

37. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

38. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

VII. INTERNETA UN E-PASTA LIETOŠANA

39. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Sabiedrības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu Sabiedrības darbību un klientiem sniegtos pakalpojumus.

40. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Sabiedrības piešķirtais epasts, ja vien valdes priekšsēdētājs nav devis citu rīkojumu.

41. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Sabiedrības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

42. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

43. Lietojot Internetu, darbinieki pārstāv Sabiedrību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

44. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Sabiedrība no darbinieka ir tiesīgs piedzīt zaudējumus, kas Sabiedrībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

45. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Sabiedrības valdes priekšsēdētājs bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

46. Sabiedrības valdes priekšsēdētājam ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem, tikai pildot amata pienākumus.

47. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.) – elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

VIII. INFORMĀCIJAS SISTĒMAS LIETOTĀJA PIEEJAS PAROLES UZBŪVE UN LIETOŠANA

48. Sabiedrības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

- 48.1. minimālam paroles garumam ir jābūt vismaz 8 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.
- 48.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 360 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.
- 48.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+).
- 48.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

49. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis Sabiedrības valdes priekšsēdētājs.

50. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

51. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Sabiedrības valdes priekšsēdētāju to izdarīt savā vietā.

52. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra ar Ctrl-Alt-Del funkcijas palīdzību, izvēloties „Lock Computer" izvēlni.

53. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Dowm =>Ok.