SIA "Rīgas nami" | Reģ. Nr. 40003109638
Rātslaukums 5, Rīga, LV-1050
T: +371 66 957 267
E: rigasnami@rigasnami.lv | www.rigasnami.lv

APSTIPRINĀTA
SIA "Rīgas nami"
2024. gada 23. janvāra
valdes sēdē
(protokols Nr. RN-2024-4/1.3-1)

SIA "RĪGAS NAMI" INFORMĀCIJAS DROŠĪBAS POLITIKA

Rīgā

2024. gada 23. janvārī Nr. RN-2024-1-pol/2.1-2

1. Lietoto terminu definīcijas

Sabiedrība	SIA "Rīgas nami", reģ.nr. 40003109638, juridiskā adrese Rātslaukums 5, Rīga, LV-1050, kas ir darba devējs ikvienam Darbiniekam.
Tiešais vadītājs	Sabiedrības pārstāvis, kurš ir norādīts attiecīgā Darbinieka darba līgumā vai iecelts ar Sabiedrības rīkojumu kā Darbinieka tiešais vadītājs.
Darbinieks	Sabiedrībā uz darba līguma pamata nodarbināta fiziska persona.
Vadība	Sabiedrības valde un/vai jebkura cita persona Sabiedrībā, kurai piešķirtas vadības funkcijas un pilnvaras.
Politika	Sabiedrības Informācijas drošības politika.
Sabiedrības klients	Fiziska, juridiska persona vai cita persona, kas jebkādā juridiski nostiprinātā veidā ir saistīta ar Sabiedrību.
Trešā puse	Fiziska, juridiska persona vai cita persona, kas nav saistīta ar Sabiedrību.
Lietotājs	Darbinieks, kurš darba vajadzībām izmanto Sabiedrības informācijas sistēmas (IS).
Lietotāja ID	Darbiniekam piešķirts unikāls identifikators – piekļuves vārds Sabiedrības IS.

2. Mērķis un apjoms

2.1. Sabiedrības informācijas drošības politikas mērķis ir pasargāt Sabiedrības darbiniekus, partnerus un klientus no nelikumīgām vai kaitējošām personu tiešām vai netiešām, apzinātām vai neapzinātām darbībām, apstrādājot informāciju un datus, kas nonāk attiecīgo personu rīcībā, kā arī lietojot noteiktu aprīkojumu savu darba pienākumu izpildes vajadzībām.

2.2. Politika regulē informācijas apstrādi jebkādās sistēmās vai jebkādos nesējos, kas iesaistīti datu/informācijas apstrādē Sabiedrībā, neatkarīgi no tā, vai datu/informācijas apstrāde ir saistīta ar Sabiedrības iekšējām komercdarbības operācijām vai Sabiedrības ārējām attiecībām ar jebkādām trešajām pusēm.

2.3. Šī Politika regulē arī to, kā Sabiedrības Darbinieki lieto viņiem pieejamo aprīkojumu un rīkus, savu darba pienākumu veikšanas ietvaros.

2.4. Politika var būt piemērojama kopā ar jebkādām citām politikām, noteikumiem, procedūrām un/vai vadlīnijām, ko periodiski pieņem un ievieš Sabiedrībā.
2.5. Jautājumi par datu aizsardzību un informācijas tehnoloģiju (turpmāk - IT) drošību Sabiedrībā, kas nav atrunāti šajā Politikā, nosūtāmi Sabiedrības personas datu aizsardzības speciālistam, e-pasts rndatuspec@rigasnami.lv.
2.6. Sabiedrībā ar šo Politiku rakstveidā iepazīstina visus Sabiedrības darbiniekus, kuriem ir apstiprināta piekļuve Sabiedrības datu apstrādes sistēmām un pārliecinās, ka viņi tos ir izpratuši. Sabiedrība organizē darbinieku apmācību vienotas un pareizas izpratnes radīšanai par IT drošības un personas datu aizsardzības jautājumiem.

3. Informācijas klasifikācija

3.1. Jebkādus fizisko personu datus, kas kļūst pieejami Darbiniekiem, veicot savus darba pienākumus, Sabiedrība uzskata par konfidenciālu informāciju, ko aizsargā šī Politika un atbilstoši piemērojamie normatīvie akti par konfidenciālu informāciju, tirdzniecības/komercnoslēpumu un personas datu aizsardzību.
3.2. Lai nodrošinātu Sabiedrības informācijas un datu aizsardzību, Sabiedrība klasificē tās pārziņā esošos datus/informāciju. Sabiedrības datus/informāciju Sabiedrība aizsargā neatkarīgi no tā, vai dati/informācija ir nonākusi Darbinieka rīcībā drukātu materiālu veidā, vai datu uzglabāšanas ierīcēs, audio/video materiālu veidā vai jebkādā citā veidā.
3.3. Sabiedrība nosaka šādu vispārīgu datu/informācijas klasifikāciju:

Kategorija	**Apraksts**	**Piemērojamības apjoms (tostarp, bet ne tikai)**
Publiski dati/ informācija	Dati/informācija, kuru var apstrādāt un izplatīt Sabiedrības iekšienē vai ārpus tās, bez jebkādas negatīvas ietekmes uz Sabiedrību, kopīgot ar jebkuru no Sabiedrības sadarbības partneriem, klientiem un /vai saistītajām pusēm.	(a) Publiski finanšu pārskati, kurus sniedz valsts iestādēm; (b) Dati/informācija, kas pieejama publiskos resursos vai ir kā citādi publiski zināma, ja vien tā nav kļuvusi publiski zināma dēļ tā, ka Darbinieks rīkojies, pārkāpjot datu/informācijas apstrādes aizsardzības prasības.

Kategorija	Apraksts	Piemērojamības apjoms (tostarp, bet ne tikai)
Iekšējās lietošanas dati/informācija	Jebkādi dati/informācija, kuru jebkāda veida lietošana, ja tas notiek, pārkāpjot piemērojamo normatīvo aktu, šīs Politikas vai jebkura cita Sabiedrības pieņemta regulējuma prasības, var kaitēt Sabiedrības un/vai jebkura tā Darbinieka, partnera, klientu interesēm.	(a) Jebkura Sabiedrības Darbinieka, struktūrvienības izstrādāti un/vai sagatavoti dokumenti, kuri nav paredzēti lietošanai Trešajai pusei; (b) Jebkādi Sabiedrības komercdarbības mērķiem izveidoti un/vai lietoti katalogi (kontaktu, informācijas, u. tml.); (c) Jebkādi iekšējie dienesta ziņojumi, paziņojumi, izziņas, slēdzieni, kas izstrādāti Sabiedrības komercdarbības vajadzībām un nav paredzēti lietošanai Trešajai pusei.
Konfidenciāli dati/informācija	Jebkādi dati/informācija, kas ir būtiska Sabiedrībai, jebkuram no tās klientiem un/vai partneriem vai saistītajām pusēm, un kuras neautorizēta apstrāde var negatīvi ietekmēt Sabiedrības, tā dalībnieku/akcionāru, klientu un/vai sadarbības partneru komercdarbību, operācijas, reputāciju, statusu kopumā, un šādas izpaušanas rezultātā jebkurai no šīm personām var tikt nodarīts nopietns kaitējums.	(a) Dati/informācija, kas Darbiniekam norādīta kā Sabiedrības komercnoslēpums, Sabiedrības datu/informācijas apstrādes sistēmu (turpmāk - IS) auditācijas pieraksti, IS rezerves kopijas; (b) Personas identifikācijas dati; (c) Informācija vai sadarbības līgumi, ko Sabiedrība ir noslēgusi savas komercdarbības gaitā, ko aizsargā konfidencialitātes vienošanās.

3.4. Atbildīgās personas par datu/informācijas apstrādi – datu/informācijas īpašnieki:
- 3.4.1. Sabiedrības IS Namejs - Sabiedrības Administratīvā departamenta Lietvedības un nodrošinājuma nodaļas vadītājs;
- 3.4.2. Sabiedrības IS Horizon - Sabiedrības Finanšu departamenta Grāmatvedības nodaļas vadītājs;
- 3.4.3. Sabiedrības IS Sharepoint – Sabiedrības Administratīvā departamenta IT nodaļas vadītājs;
- 3.4.4. Sabiedrības IS Weeze - Sabiedrības Administratīvā departamenta IT nodaļas vadītājs;
- 3.4.5. Sabiedrības IS – tīmekļa mājas lapa – Sabiedrības rīkojumā noteiktās personas.

4. Datu/informācijas apstrādē iesaistītās sistēmas

4.1. Jebkādas IS, tostarp, bet ne tikai datortehnika, jebkāda veida programmatūra, operētājsistēmas, jebkādas datu/informācijas uzglabāšanas vides, IS lietotāju identifikācijas, autentifikācijas tīkla konti, elektroniskā pasta konti, tīmekļa pārlūkprogrammas un jebkāda cita programmatūra un rīki, ko izmanto Sabiedrības darbībā, uzskatāmi par Sabiedrības īpašumu.

4.2. Ikvienam Darbiniekam ir pienākums lietot Sabiedrības IS un rīkus ar pienācīgu rūpību un uzmanību, un tikai ar Sabiedrības komercdarbību saistītiem mērķiem, Darbiniekam piešķirto piekļuves tiesību ietvaros.

5. Darbinieku pienākumi

5.1. Jebkādi dati/informācija, kas nonāk Darbinieka rīcībā, pildot darba pienākumus, lietojami, ievērojot datu/informācijas klasifikācijā noteikto aizsardzību saskaņā ar šo Politiku, tos aizliegts izpaust vai nodot jebkādai Trešajai pusei, kamēr un ja vien Vadība nepaziņo, ka šādi dati/informācija ir kļuvusi publiska, vai ir kā citādi pārklasificēta par informāciju, kas vairs netiek aizsargāta šajā Politikā paredzētajā kārtībā.

5.2. Visus personas datus un citu informāciju, ar kuras palīdzību var identificēt fizisku personu, Darbinieks apstrādā tikai, ja tas ir nepieciešams Sabiedrībai un ciktāl tas ir nepieciešams Darbinieka darba pienākumu veikšanas nolūkā, ar nosacījumu, ka šādas darbības tiek veiktas Darbiniekam piešķirto pilnvaru robežās un saskaņā ar likumā paredzētajām datu aizsardzības prasībām (jo īpaši, saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)).

5.3. Jebkādus datu/informācijas pieprasījumus un/vai pieprasījumus par datu/informācijas apstrādi, ko Darbinieks, veicot savus darba pienākumus, ir saņēmis no datu īpašniekiem – fiziskām personām, Darbiniekam nekavējoties jāpārsūta turpmākai izskatīšanai Darbinieka Tiešajam vadītājam un Sabiedrības personas datu aizsardzības speciālistam.

5.4. Ikvienam Darbiniekam ir pienākums ievērot šo Politiku, kā arī pildīt spēkā esošo vietējo, reģionālo vai starptautisko normatīvo aktu prasības, kas paredz informācijas/datu apstrādes un aizsardzības nosacījumus. Politikas neievērošanu uzskata par būtisku noteiktās darba kārtības pārkāpumu un tā rezultātā, pēc Sabiedrības ieskatiem, Darbiniekam var piemērot disciplinārsodu vai atlaist Darbinieku no darba. Tas tāpat var izraisīt pārkāpumu pieļāvušā Darbinieka saukšanu pie administratīvās vai kriminālās atbildības.

5.5. Darbinieka pienākums ir regulāri dzēst nevajadzīgos e-pasta sūtījumus Sabiedrības pārziņā esošajā e-pasta IS, kā arī tos e-pasta sūtījumus, kas ir vecāki par 12 mēnešiem. Darbinieka pienākumu izpildē vajadzīgos e-pasta sūtījumus nepieciešamības gadījumā Darbinieks var uzglabāt Sabiedrības nodrošinātajā darba datorā.

6. Piekļuves un aizsardzības pārvaldība

6.1. Sabiedrības IS Darbinieks drīkst piekļūt no Sabiedrības nodrošināta datora, ierīces, ja tas nepieciešams Darbinieka darba pienākumu veikšanai Darbiniekam piešķirto piekļuves tiesību ietvaros. Darbiniekam piešķirtās piekļuves tiesības Sabiedrības IS nenozīmē, ka Darbinieks ir pilnvarots apskatīt vai lietot visus Sabiedrības IS glabātos datus/informāciju.

6.2. Darbinieka lietotāja ID ir unikāls un identificē konkrētu Darbinieku. Ikviens Darbinieks atbild par visām darbībām, kas veiktas ar Darbinieka lietotāja ID kontu, līdz ar to, primārais Darbinieka pienākums ir nodrošināt, lai Darbinieka ID nebūtu pieejams Trešajai pusei un citiem Darbiniekiem, ja vien Sabiedrība nav noteikusi citu kārtību.

6.3. Sabiedrības IS lietotāju identifikācijai, autentifikācijai atļauts pielietot IS lietotāju daudzfaktoru autentifikācijas risinājumus.

6.4. Sabiedrības IS nodrošina IS lietotāja paroles veidošanu ar pienācīgu rūpību, izmantojot paroļu veidošanas nosacījumus, lai tās nav iespējams viegli atminēt, tās sastāv vismaz no 12 simboliem (tai skaitā, lielajiem un mazajiem burtiem, cipariem, kā arī speciālajiem simboliem), tās neietver personas datus un tās tiek regulāri mainītas ne retāk kā vienu reizi 3 (trīs) mēnešos. Ikviens Darbinieks personīgi atbild par tam piešķirtā Sabiedrības IS lietotāja paroles atbilstību šai Politikai un jebkādiem citiem Sabiedrības noteikumiem.

6.5. Darbinieks drīkst piekļūt Sabiedrības konfidenciāliem datiem/informācijai tikai tad, ja šādas pilnvaras ir paredzētas attiecīgā Darbinieka darba līgumā, un/vai, ja Sabiedrība ir īpaši piešķīrusi Darbiniekam šādas pilnvaras.

6.6. Sabiedrībai izbeidzot darba attiecības ar Darbinieku, Darbinieka piekļuves tiesības tiek anulētas Darbinieka pēdējā darba dienā.

7. Drošības pasākumi

7.1. Sabiedrības IS visiem jebkādā formā (drukātā, elektroniskā, u.tml.) iegūtiem un apstrādātiem datiem/informācijai piemērojamas šīs Politikas un jebkāda normatīvā regulējuma prasības attiecībā uz datu/informācijas iegūšanu, apstrādi, aizsardzību un uzglabāšanu, un šādus dokumentus uzglabā Sabiedrības norādītā, drošā vietā ar tādu uzglabāšanas termiņu, kādu paredz piemērojamie likumi un/vai nosaka Sabiedrība.

7.2. Darbiniekiem aizliegts glabāt jebkādus konfidenciālus datus/informāciju savās ierīcēs, izņemot informāciju, kas ir īslaicīgi nepieciešama konkrētai, ar darba pienākumu pildīšanu saistītai darbībai. Visa nepieciešamā konfidenciālā un personu identificējošā informācija jāuzglabā tikai Sabiedrības IT personāla apstiprinātā mākoņa krātuvē un Sabiedrības iekštīklā. Darbiniekam pēc iespējas ir jāizvairās no jebkādas šādu datu lejupielādēšanas vietējās ierīcēs un tas jādara tikai tādā gadījumā, ja tas ir pamatoti nepieciešams informācijas apstrādei konkrētai, ar darba pienākumu pildīšanu saistītai darbībai.

7.3. Sabiedrības pilnvarotam IT personālam ir tiesības apstrādāt, filtrēt un pārraudzīt Sabiedrības Darbinieku piekļuvi Interneta resursiem un to veiktās darbības Internetā no Sabiedrības iekštīkla saskaņā ar piemērojamo normatīvo aktu prasībām.

7.4. Sabiedrības pilnvarotam IT personālam ir tiesības piekļūt Sistēmas lietotāja Sabiedrības piešķirtā datorā glabātajiem dokumentiem un informācijai, ja tas nepieciešams Sabiedrības funkciju izpildei saskaņā ar piemērojamo normatīvo aktu prasībām.

7.5. Jebkurām mobilajām, portatīvajām ierīcēm (tostarp, klēpjdatoriem, planšetēm, viedtālruņiem un citām plaukstdatoru ierīcēm), kā arī jebkādām mākoņa informācijas uzglabāšanas vietām jābūt apstiprinātām no Sabiedrības IT personāla puses un pienācīgi aizsargātām, lai novērstu neautorizētu piekļuvi.

7.6. Darbiniekam piešķirtajā aprīkojumā un rīkos tikai Sabiedrības IT nodaļas speciālistiem atļauts uzstādīt tikai Sabiedrības licencētas un apstiprinātas sistēmas un programmatūru. Citas programmatūras uzstādīšana, šajā Politikā aprakstīto mērķu sasniegšanai, jāsaskaņo ar Sabiedrības IT nodaļu.

7.7. Darbiniekam, lietojot personīgās (mājas) ierīces, lai piekļūtu Sabiedrības IS (piemēram, elektroniskais pasts, tiešsaistes/mākoņa datubāzes), ir pienākums ievērot šīs Politikas prasības tieši tāpat kā ja viņi lietotu Sabiedrības nodrošināto aprīkojumu. Līdz ar to, personīgajā ierīcē ir aizliegts glabāt jebkādus ar Sabiedrību saistītus datus/informāciju, jebkāda datu/informācijas apstrāde ir pieļaujama tikai ar Sabiedrības lietoto mākoņa un tiešsaistes glabāšanas vietu starpniecību.

7.8. Darbiniekam ir aizliegts izmantot publiskas piekļuves ierīces (piemēram, datorus, u.c. portatīvās ierīces publiskās interneta kafejnīcās, bibliotēkās, u.tml.), lai piekļūtu Sabiedrības IS.

7.9. Gadījumā, ja Darbiniekam apstiprina piekļuves tiesības pie Sabiedrības klienta IS, Darbiniekam ir pienākums lietot Sabiedrības klienta vai sadarbības partnera piešķirtos piekļuves rekvizītus un ievērot šīs Politikas un Sabiedrības klienta sniegtos norādījumus par drošas datu/informācijas apstrādes prasībām (tostarp, šifrēšanas sistēmu, paroļu lietošanu, datu lietošanas ierobežojumu, īpaši paredzētas atrašanās vietas lietošanu, u.tml.).

7.10. Tiklīdz, pēc Sabiedrības iekšējiem un/vai ārējiem normatīvajiem aktiem, Sabiedrības valdījumā esošie Konfidenciālie dati/informācija vairs nav nepieciešami Sabiedrības darbībai, Sabiedrība šādus datus/informāciju dzēš, iznīcina visas to kopijas, un attiecīgo datu/informācijas apstrādē iesaistītos Darbiniekus informē par viņu pienākumu dzēst/iznīcināt, vai arī nodot atpakaļ Sabiedrībai datus/informāciju, kas Darbiniekam vairs nav nepieciešami savu darba pienākumu veikšanai.

7.11. Ja ar Darbinieku tiek izbeigtas darba tiesiskās attiecības Darbinieka pienākums ir atdot atpakaļ Sabiedrībai darba pienākumu izpildē Darbiniekam izsniegtajā Sabiedrības datorā izveidotos, uzglabātos datus/informāciju, programmatūru un visus tehniskos resursus.

7.12. Darbinieks bez Sabiedrības vadības saskaņojuma nenosūta, nepārsūta un nekādā citā veidā nenodod Trešajai pusei šajā Politikā minēto datus/informāciju, ja vien tas nav nepieciešams Darbinieka darba pienākumu izpildei, un tikai ciktāl tas ir nepieciešams šādu pienākumu

izpildei. Gadījumā, ja Darbiniekam Sabiedrības pārziņā esošie dati/informācija ir jāpārsūta vai jāiesniedz Trešajai pusei, tad Darbiniekam ir noteikti jānodrošina pārsūtāmo datu/informācijas aizsardzība un jāveic visi Sabiedrības noteiktie datu/informācijas apstrādes aizsardzības pasākumi.

7.13. Sabiedrības Administratīvā departamenta Kvalitātes un riska vadītājam sadarbojoties ar Administratīvā departamenta IT nodaļu ir pienākums veikt Sabiedrības IS risku analīzi gan pirms Sabiedrības IS ekspluatācijas sākšanas, gan arī tās ekspluatācijas laikā regulāri vismaz reizi gadā un sagatavo Sabiedrības IS drošības risku pārvaldības plānu.

7.14. Riska analīzē vērtē zināmo apdraudējumu iestāšanās iespējamību un apdraudējuma iestāšanās gadījumā iespējamo ietekmi uz Sabiedrības uzdevumu izpildi, lai aprēķinātu drošības risku un sagatavotu rakstisku Sabiedrības IS drošības risku pārvaldības plānu.

7.15. Sabiedrības IS drošības risku pārvaldības plānā norāda drošības riska mazināšanas pasākumus, izpildes termiņu, nepieciešamos resursus ikvienam Sabiedrības IS drošības risku pārvaldības plānā norādītajam apdraudējumam.

7.16. Izpildot Sabiedrības IS drošības risku pārvaldības plānā norādītos drošības risku mazināšanas pasākumus, tiek sasniegts Sabiedrībai pieņemams drošības riska līmenis.

7.17. Sabiedrība auditē datu/informācijas apstrādē pielietotās sistēmas, lai kontrolētu nepārtrauktu atbilstību šai Politikai un piemērojamajām normatīvajām prasībām.

7.18. IT nodaļas pienākumi ietver regulāru Sabiedrības IS un tīkla notikumu reģistrēšanu un uzraudzību.

8. Aizliegtās darbības

8.1. Izņemot īpaši paredzētus izņēmumus, Sabiedrībai, tā klientiem vai sadarbības partneriem piederošu aprīkojumu, sistēmas vai rīkus nekādā gadījumā un nekādos apstākļos nedrīkst izmantot ar Darbinieka darba pienākumiem vai ar Sabiedrības darbību nesaistītiem mērķiem.

8.2. Turpmāk minētās darbības ir Sabiedrībā stingri aizliegtas, bez izņēmumiem:

8.2.1. Jebkuras personas vai Sabiedrības ar intelektuālā īpašuma tiesībām aizsargātu tiesību pārkāpšana, tostarp, bet ne tikai jebkādas nelegālas programmatūras, tiešsaistes platformu, jebkādu citu elektronisko saturu, kurus Sabiedrība nav licencēta lietot, uzstādīšana, kopēšana, izplatīšana vai uzglabāšana jebkādās Sabiedrības sistēmās vai aprīkojumā;

8.2.2. Ar autortiesībām aizsargātu materiālu neautorizēta kopēšana;

8.2.3. Jebkuras personas tiesību aizskaršana, pārmērīgi un bez vajadzības ievācot un apstrādājot attiecīgā subjekta personas datus;

8.2.4. Piekļuve datiem, serverim vai kontam tādiem mērķiem, kas nav saistīti ar Sabiedrības komercdarbību vai attiecīgā Darbinieka darba pienākumu veikšanu;

8.2.5. Programmatūras, tehniskās informācijas, šifrēšanas programmatūras vai tehnoloģijas eksportēšana, pārkāpjot piemērojamos starptautiskos vai nacionālos normatīvos aktus un/vai Sabiedrības norādījumus;

8.2.6. Jebkādu datu vai informācijas, kurai ir īpašuma un/vai konfidenciāla vērtība Sabiedrībai, eksportēšana, ja šāda eksportēšana nav nepieciešama Sabiedrības komercdarbības vai Darbinieka darba pienākumu veikšanas gaitā, un/vai, ja tā pārkāpj Sabiedrības iekšējos noteikumus, piemērojamos normatīvos aktus;

8.2.7. Darbinieka konta paroles atklāšana citām personām un citu personu pielaišana lietot šādu kontu (tostarp, bet neaprobežojoties ar Darbinieka ģimenes locekļiem);

8.2.8. Krāpniecisku produkcijas, preču vai pakalpojumu piedāvājumu izveide, izmantojot Sabiedrības kontu;

8.2.9. Tīkla sakaru drošības pārkāpumu vai pārtraukumu īstenošana. Šādi drošības pārkāpumi iekļauj, bet tie neaprobežojas ar piekļuvi datiem, ja Darbinieks nav to paredzētais saņēmējs, vai pierakstīšanos serverī vai kontā, kuram Darbinieks nav skaidri pilnvarots piekļūt, ja vien šādas piekļuves tiesības nav piešķirtas Darbiniekam saistībā ar attiecīgā Darbinieka dalību konkrētā Sabiedrības projektā;

8.2.10. Jebkādas programmas/skripta/komandas lietošana vai jebkāda veida ziņojuma nosūtīšana, ar nolūku ar jebkādiem līdzekļiem traucēt vai atspējot lietotāja darba sesiju.

9. Lietotāju tiesību pārvaldība

9.1. Sabiedrības IT nodaļa saņem no Personāla nodaļas un/vai struktūrvienības vadītāja informāciju un/vai Sabiedrības darbinieka (saskaņojot ar tiešo vadītāju) informāciju par piekļuvi nepieciešamajiem IS resursiem.

9.2. Informācija par jauna Darbinieka pievienošanu/anulēšanu IS resursiem, kas iesniegta pēc pieprasījuma no Personāla nodaļas (vai citos gadījumos) tiek uzglabāta divus gadus pēc lietošanas tiesību piešķiršanas/anulēšanas vai līdz brīdim, kad Lietotājam vairāk nav nepieciešamas piekļuves tiesības.

9.3. Par Sabiedrības IS Lietotāju tiek apstiprinātas personas, kuras ir iepazīstinātas ar šo Politiku, un kurām ir sniegta piekļuve Sabiedrības IS.

9.4. Sabiedrība IS Lietotāju tiesības tiek nodrošinātas pēc pieprasījuma, atbilstoši Darbinieka amata aprakstā noteikto tiešo darba pienākumu izpildei.

9.5. Ne retāk kā reizi gadā Sabiedrības IT nodaļa veic Lietotājiem piešķirto tiesību auditu.

9.6. Lietotājam piešķirtās tiesības darba pienākumu veikšanai ir derīgas tikai uz periodu, kurā Lietotājam nepieciešama atbilstošā piekļuve.

9.7. Sabiedrības IT nodaļa sniedz detalizētu informāciju Sabiedrības IS Lietotājam par IS funkcionalitāti un Lietotājam piešķir:

9.7.1. Sabiedrības IS Lietotāja identifikatoru (ID);

9.7.2. vienreiz lietojamu Sabiedrības IS Lietotāja paroli - sākotnējo paroli, ko Lietotājam nepieciešams nomainīt pie pirmās autorizēšanās IS;

9.7.3. piekļuvi pie Sabiedrības IS atbilstoši pieprasījumā noteiktajam apjomam.

9.8. Sabiedrības IS Lietotājs, saņemot autorizācijas datus, veic autorizēšanos Sabiedrības IS, un pie pirmās autorizācijas veic izsniegtās sākotnējās paroles nomaiņu. Ja Lietotāja autorizācija ir neveiksmīga, Lietotājs sazinās ar Sabiedrības IT nodaļu par atkārtotu sākotnējās paroles izsniegšanu.

9.9. Sabiedrības IT nodaļa, saņemot pieteikumu vai konstatējot faktu par Lietotāja tiesību anulēšanas nepieciešamību, veic darbības, lai anulētu Lietotājam piešķirtās piekļuves tiesības Sabiedrības IS.

9.10. Sekmīgi veicot Lietotāja tiesību anulēšanas procesu, Sabiedrības IT nodaļa aktualizē informāciju pieejas tiesību reģistrā.

9.11. Pēc Lietotāja tiesību anulēšanas Sabiedrība uzglabā informāciju (darba e-pasti un lietotāja profila darba failus) 90 dienas, ja netiek noteikts savādāk ar atsevišķu Sabiedrības rīkojumu.

10. Ziņošana par drošības incidentiem

10.1. Par visiem datu/informācijas apstrādes drošības incidentiem vai iespējamiem incidentiem Darbiniekam nekavējoties ir jāziņo savam tiešajai vadītājam, Sabiedrības IT nodaļai un Sabiedrības personas datu aizsardzības speciālistam, kuri organizē, veic nepieciešamos pasākumus iespējamā kaitējuma novēršanai, radītā kaitējuma seku likvidēšanai un iepriekšējā drošības stāvokļa atjaunošanai.

10.2. Pēc informācijas saņemšanas no 10.1.punktā norādītajiem speciālistiem, Sabiedrības vadība personas datu aizsardzības pārkāpuma gadījumā, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums kļuvis zināms, paziņo par personas datu aizsardzības pārkāpumu uzraudzības iestādei, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām.

10.3. Sabiedrība dokumentē visus personas datu aizsardzības pārkāpumus, saglabājot faktus, kas saistīti ar personas datu pārkāpumu, tā radītajām sekām un veiktajām koriģējošām darbībām.

11. Noslēguma jautājumi

11.1. Lai nodrošinātu efektīvu Politikas piemērošanu, Sabiedrība regulāri veic Politikas ieviešanas uzraudzību un pēc nepieciešamības, bet ne retāk kā vienu reizi gadā pārskata Politiku un vajadzības gadījumā veic attiecīgas izmaiņas.

11.2. Sabiedrība nodrošina Darbinieku iepazīstināšanu ar Politiku Sabiedrībā noteiktajā kārtībā. Politika ir pieejama Sabiedrības dokumentu vadības informācijas sistēmā.