GAŖS
Latgales Vēstniecība

SIA "Austrumlatvijas koncertzāle"
Reģ. nr. 42403026217
Pils iela 4, Rēzekne, LV-4601
+371 22020206 | koncertzale@rezekne.lv

SIA "Austrumlatvijas koncertzāle"

Valdes locekle _____ Diāna Zirniņa

2018. g. „25." maijs

INFORMĀCIJAS DROŠĪBAS POLITIKA

Saturs

1. Lietoto terminu definīcijas

Uzņēmums	SIA "Austrumlatvijas koncertzāle", reģistrācijas Nr. 42403026217, juridiskā adrese Pils iela 4, Rēzekne, kas ir darba devējs ikvienam darbiniekam, kurš ir nodarbināts uz Darba līguma pamata.
Tiešais vadītājs	Uzņēmuma pārstāvis, kurš ir norādīts attiecīgā Darbinieka Amata aprakstā, Darba līgumā vai iecelts ar Uzņēmuma rīkojumu kā Darbinieka tiešais vadītājs.
Darbinieks	Uzņēmuma nodarbināta fiziska persona.
Vadība	Valde, rīkotājdirektors un/vai jebkura cita persona Uzņēmumā, kurai piešķirtas vadības funkcijas un pilnvaras.
Politika	Šī Informācijas drošības politika.
Trešā puse	Fiziska persona, juridiska persona vai cita persona, kas nav saistīta ar Uzņēmumu.

2. Mērķis un apjoms

2.1. Uzņēmuma informācijas drošības sistēmas mērķis ir pasargāt Uzņēmuma 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 Uzņēmumā, neatkarīgi no tā, vai datu/informācijas apstrāde ir saistīta ar Uzņēmuma iekšējām komercdarbības operācijām vai Uzņēmuma ārējām attiecībām ar jebkādām trešajām pusēm.

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

2.5. Ar visiem informācijas drošības sistēmas jautājumiem un informācijas/datu drošības jautājumiem, kas nav atrunāti šajā Politikā, jāvēršas pie Uzņēmuma datu aizsardzības speciālista.

3. Informācijas klasifikācija

3.1. Jebkādu informāciju/datus, kas kļūst pieejami Darbiniekiem, veicot savus darba pienākumus, ja šāda informācija/dati ir saistīti ar Uzņēmumu un tā darbību, klientiem vai sadarbības partneriem, uzskata par Uzņēmumam piederošu un konfidenciālu informāciju, ko, līdz ar to, aizsargā atbilstoši piemērojamie normatīvie akti par konfidenciālas informācijas, tirdzniecības/komercnoslēpumu un personas datu aizsardzību.

3.2. Lai nodrošinātu pienācīgu informācijas un datu aizsardzību, Uzņēmums veic iekšējo informācijas klasifikāciju. Informāciju/datus aizsargā neatkarīgi no tā, vai šāda informācija ir nonākusi Darbinieka rīcībā drukātu materiālu veidā, jebkādās datu uzglabāšanas ierīcēs, audio/video materiālu veidā vai jebkādā citā veidā.

3.3. Uzņēmums lieto šādu vispārīgu informācijas klasifikāciju:

Kategorija	**Apraksts**	**Piemērojamības apjoms (tostarp, bet ne tikai)**
Publiska informācija	Informācija, kuru var apstrādāt un izplatīt Uzņēmuma iekšienē vai ārpus tā, bez jebkādas negatīvas ietekmes uz Uzņēmumu, jebkuru no tā partneriem, klientiem un /vai saistītajām pusēm.	(a) Publiski finanšu pārskati, kurus sniedz valsts iestādēm; (b) Informācija, kas pieejama publiskos resursos vai ir kā citādi publiski zināma, ja vien tā nav kļuvusi publiski zināma dēļ tā, ka Darbinieks rīkojies, pārkāpjot informācijas/datu drošības prasības.
Iekšējā informācija	Jebkāda informācija, kuras jebkāda veida lietošana, ja tas notiek, pārkāpjot piemērojamo normatīvo aktu, šīs Politikas vai jebkura cita Uzņēmuma pieņemta regulējuma prasības, var kaitēt Uzņēmuma un/vai jebkura tā Darbinieka, partnera, klientu interesēm.	(a) Jebkura Uzņēmuma Darbinieka, struktūrvienības izstrādāti un/vai sagatavoti dokumenti; (b) Jebkādi Uzņēmuma komercdarbības mērķiem izveidoti un/vai lietoti katalogi (kontaktu, informācijas, u. tml.); (c) Jebkādi iekšēji dienesta ziņojumi, paziņojumi, izziņas, slēdzieni, kas izstrādāti Uzņēmuma komercdarbības vajadzībām.
Konfidenciāla informācija	Jebkāda informācija, kas ir tik būtiska Uzņēmumam, jebkuram no tā klientiem un/vai partneriem vai saistītajām pusēm, kuras neautorizēta izpaušana var negatīvi ietekmēt Uzņēmuma, 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) Politikas, procedūras, iekšējie noteikumi, vadības lēmumi; (b) Informācija, kas Darbiniekam norādīta kā Uzņēmuma komercnoslēpums; (c) Cita finanšu, cilvēkresursu, juridiskas, mārketinga dabas informācija, pārdošanas procedūras, plāni un operācijas; (d) Biznesa, produkcijas plāni; (e) Personas identifikācijas dati; (f) Informācija, ko aizsargā katra Darbinieka parakstīta konfidencialitātes vienošanās; (g) Informācija, ko aizsargā konfidencialitātes vienošanās vai

		sadarbības līgumi, ko Uzņēmums ir noslēdzis savas komercdarbības gaitā.

4. Datu/informācijas apstrādē iesaistītās sistēmas

4.1. Jebkādas informācijas sistēmas, tostarp, bet ne tikai datortehnika, jebkāda veida programmatūra, operētājsistēmas, jebkādas uzglabāšanas vides, tīkla konti, elektroniskā pasta konti, pārlūku sistēmas un jebkāda cita tehniskā bāze un rīki, ko izmanto Uzņēmuma darbībā, uzskatāmi par Uzņēmuma īpašumu.

4.2. Ikvienam Darbiniekam ir pienākums lietot šādu tehnisko aprīkojumu un rīkus ar pienācīgu rūpību un uzmanību, un tikai ar Uzņēmuma komercdarbību saistītiem mērķiem. Vienīgais izņēmums ir gadījumi, kad Uzņēmums ir piešķīris Darbiniekam tehnisko aprīkojumu (piemēram, mobilā tālruņa ierīci), sniedzot skaidru piekrišanu to lietot arī personīgām vajadzībām.

4.3. Datu/informācijas apstrāde Uzņēmumā tiek veikta gan tehniski, gan elektroniski, gan manuāli – izmantojot ar tehniskiem parametriem neapveltītus līdzekļus (papīrs, pildspalva u.tml.).

5. Darbinieku pienākumi

5.1. Jebkāda informācija/dati, kas nonāk Darbinieka rīcībā, pildot savus darba pienākumus, uzskatāmi par konfidenciāliem un lietojami kā konfidenciāli, ievērojot to aizsardzību saskaņā ar šo Politiku, un tos neizpauž nekādām trešajām pusēm, kamēr un ja vien Vadība nepaziņo, ka šāda 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, ievāc un apstrādā tikai, ja tas ir nepieciešams 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 pieprasījumus un/vai pieprasījumus par datu apstrādi, ko Darbinieks, veicot savus darba pienākumus, ir saņēmis no datu īpašniekiem – fiziskām personām, nekavējoties pārsūta turpmākai izskatīšanai Vadībai.

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 Uzņēmuma ieskatiem, Darbiniekam var piemērot disciplinārsodu vai atlaist Darbinieku no darba. Tas tāpat var izraisīt pārkāpumu pieļāvušā Darbinieka saukšanu pie administratīvās vai krimināls atbildības.

6. Piekļuves un aizsardzības pārvaldība

6.1. Darbinieki var piekļūt jebkādām Darbiniekiem pieejamām ierīcēm, ja tas nepieciešams attiecīgo Darbinieku darba pienākumu veikšanas vajadzībām, atbildības ietvaros un uz zinātvajadzības pamata. Piekļuves tiesības jebkādai sistēmai nenozīmē, ka Darbinieks ir pilnvarots apskatīt vai lietot visu attiecīgajā sistēmā esošo informāciju.

6.2. Izmantotie lietotāja ID ir unikāli un identificē konkrētu Darbinieku. Ikviens Darbinieks atbild par visām darbībām kas saistītas ar viņa/viņas personīgo ID kontu, līdz ar to, primārais pienākums ir nodrošināt, lai Darbinieka ID nebūtu pieejams nekādām trešajām pusēm un pat ne citiem Darbiniekiem, ja vien Uzņēmums nav noteicis citu kārtību.

6.3. Sistēmas drošības paroles izveido ar pienācīgu rūpību, ar nosacījumu, ka tās nevar viegli atminēt, tās neietver personas datus un tās tiek regulāri mainītas (vismaz reizi 3 (trīs) mēnešos). Ikviens Darbinieks personīgi atbild par savas drošības paroles atbilstību šai Politikai un jebkādiem citiem Uzņēmuma noteikumiem.

6.4. Darbinieks piekļūst konfidenciālai informācijai /datiem tikai, ja šādas pilnvaras ir paredzētas attiecīgā Darbinieka Darba līgumā, un/vai ja Uzņēmums ir piešķīris Darbiniekam šādas pilnvaras.

7. Drošības pasākumi

7.1. Visiem jebkādā formā (drukātā, elektroniskā, u.tml.) ievāktiem un apstrādātiem datiem un informācijai piemērojamas šīs Politikas un jebkāda normatīvā regulējuma prasības attiecībā uz datu/informācijas ievākšanu, apstrādi, aizsardzību un uzglabāšanu, un šādus dokumentus uzglabā Uzņēmuma norādītā, drošā vietā ar tādu uzglabāšanas termiņu, kādu paredz piemērojamie likumi un/vai norāda Uzņēmums.

7.2. Darbiniekiem aizliegts glabāt jebkādu konfidenciālu informāciju savās ierīcēs, izņemot informāciju, kas ir īslaicīgi nepieciešama konkrētai, ar darbu saistītai darbībai. Visa nepieciešamā konfidenciālā un personīgi identificējamā informācija jāuzglabā tikai Uzņēmuma IT personāla apstiprinātā mākoņa krātuvē un Uzņēmuma iekštīklā. Ir jāizvairās no jebkādas šādu datu lejupielādēšanas vietējās ierīcēs un tas jādara tikai, ja tas ir pamatoti nepieciešams saistībā ar informācijas apstrādi darba vajadzībām.

7.3. Pienācīgi pilnvarots Uzņēmuma IT personāls ir tiesīgs filtrēt un pārraudzīt Darbinieku interneta piekļuvi un Darbinieku internetā veiktās darbības saskaņā ar piemērojamo normatīvo aktu prasībām.

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

7.5. Uzņēmumā lietotajā aprīkojumā un rīkos var instalēt un lietot tikai Uzņēmuma licencētas un autorizētas sistēmas un programmatūru. Pirms jebkādas programmatūras lejupielādēšanas vai instalēšanas Darbiniekiem piederošās un lietotās ierīcēs šajā Politikā aprakstītajiem mērķiem, ir jāsaņem IT personāla atļauja.

7.6. Gadījumos, kad Darbinieki lieto personīgās (mājas) ierīces, lai piekļūtu Uzņēmuma korporatīvajiem resursiem (piemēram, klientu attiecību pārvaldības (CRM) programma, elektroniskais pasts, tiešsaistes / mākoņa datubāzes), Darbiniekiem ir pienākums ievērot šīs Politikas prasības tieši tāpat kā ja viņi lietotu Uzņēmuma nodrošināto aprīkojumu. Līdz ar to, ierīcē ir aizliegts glabāt jebkādus ar Uzņēmumu saistītus datus un informāciju; jebkāda datu apstrāde ir pieļaujam tikai ar Uzņēmuma lietoto mākoņa un tiešsaistes glabāšanas vietu starpniecību.

7.7. Jebkurā gadījumā, ir stingri aizliegts izmantot publiskas piekļuves ierīces (piemēram, interneta kafejnīcās, bibliotēkās, u.tml.), ja vien tas nav kritiski un steidzami nepieciešams saistībā ar darbu un Darbinieka Tiešais vadītājs ir sniedzis skaidru rakstveida piekrišanu šādai darbībai.

7.8. Gadījumā, ja Darbiniekam tiek piešķirtas tiesības piekļūt Uzņēmuma klienta vai sadarbības partnera datņu glabāšanas sistēmai, Darbiniekam ir pienākums lietot klienta vai partnera piešķirtos piekļuves

rīkus un ievērot sniegtos norādījumus par drošas informācijas/datu apstrādes prasībām (tostarp, šifrēšanas sistēmu, paroļu lietošana, datu lietošanas ierobežojumi, īpaši paredzētu atrašanās vietu lietošana, u.tml.).

7.9. Tiklīdz, pēc Uzņēmuma ieskatiem, aizsargātie dati/informācija vairs nav nepieciešama Uzņēmuma darbībai, šādus datus/informāciju dzēš, uznīcina visas to kopijas, un attiecīgās informācijas /datu apstrādē iesaistītos Darbiniekus attiecīgi informē par viņu pienākumu dzēst/iznīcināt un nodot atpakaļ Uzņēmumam informāciju/datus, kas viņiem vairs nav nepieciešami savu darba pienākumu veikšanai, un, jo īpaši, atdot atpakaļ Uzņēmumam, dzēst un iznīcināt kopijas, ja ar attiecīgo Darbinieku tiek izbeigtas darba tiesiskās attiecības.

7.10. Nekādu šajā Politikā minēto informāciju/datus nenosūta, nepārsūta un nekādā citā veidā neiesniedz Trešajai pusei, ja vien tas nav nepieciešams Darbinieka darba pienākumu izpildei, un tikai ciktāl tas ir nepieciešams šādu pienākumu izpildei. Gadījumā, ja datus pārsūta vai iesniedz Trešajām pusēm, ir noteikti jānodrošina datu aizsardzība un jāveic visi atbilstošie drošības pasākumi.

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

7.12. Pasākumi, kas veicami tehnisko resursu aizsardzībai:

7.12.1. pret ugunsgrēku – ierīkota signalizācija;

7.12.2. pret pārkaršanu – ierīkoti temperatūras mērītāji;

7.12.3. pret sprieguma izmaiņām elektroniskajos tīklos – ierīkoti nepārtrauktās barošanas avoti, kas nodrošina tehniskā resursa darbību pēc elektriskās strāvas padeves pārtraukšanas uz vienu stundu;

7.12.4. pret trešās personas ļaunprātīgu rīcību – nodrošināta pieejas kontrole.

8. Aizliegtās darbības

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

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

(a) Jebkuras personas vai uzņēmuma ar intelektuālā īpašuma tiesībām aizsargātu tiesību pārkāpšana, tostarp, bet ne tikai jebkādas nelegālas programmatūras, tiešsaistes platformu, jebkādu citu elektronisko saturu, kurus Uzņēmums nav licencēts lietot, uzstādīšana, kopēšana, izplatīšana vai uzglabāšana jebkādās Uzņēmuma sistēmās vai aprīkojumā;

(b) Ar autortiesībām aizsargātu materiālu neautorizēta kopēšana;

(c) Jebkuras personas tiesību aizskaršana, pārmērīgi un bez vajadzības ievācot un apstrādājot attiecīgā subjekta personas datus;

(d) Piekļuve datiem, serverim vai kontam tādiem mērķiem, kas nav saistīti ar Uzņēmuma komercdarbību vai attiecīgā Darbinieka darba pienākumu veikšanu;

(e) Programmatūras, tehniskās informācijas, šifrēšanas programmatūras vai tehnoloģijas eksportēšana, pārkāpjot piemērojamos starptautiskos vai nacionālos normatīvos aktus un/vai Uzņēmuma norādījumus;

(f) Jebkādu datu vai informācijas, kurai ir īpašuma un/vai konfidenciāla vērtība Uzņēmumam, eksportēšana, ja šāda eksportēšana nav nepieciešama Uzņēmuma komercdarbības vai Darbinieka darba

pienākumu veikšanas gaitā, un/vai, ja tā pārkāpj Uzņēmuma iekšējos noteikumus, piemērojamos normatīvos aktus;

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

(h) Krāpniecisku produkcijas, preču vai pakalpojumu piedāvājumu izveide, izmantojot Uzņēmuma kontu;

(i) 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 Uzņēmuma projektā;

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

9. Ziņošana par drošības incidentiem

9.1. Par visiem informācijas/datu apstrādes drošības incidentiem vai iespējamiem incidentiem nekavējoties ir jāziņo Vadībai, kura, attiecīgi, veic visus pasākumus iespējamā kaitējuma novēršanai, radītā kaitējuma seku likvidēšanai un iepriekšējā drošības stāvokļa atjaunošanai.

9.2. Ja piemērojams, Vadībai ir pienākums nodrošināt turpmāku ziņošanu par datu/informācijas drošības pārkāpumu iestādēm un iesaistītajām fiziskajām personām, kā to paredz piemērojamie normatīvie akti un/vai Eiropas Savienības likumi.

Sagatavoja:
Pasākumu producente Daira Lāce _____

Personāla speciāliste – pasākumu un konferenču organizatore Agita Papkova _____