INFORMĀCIJAS DROŠĪBAS POLITIKA

Rīgā, 2018.gada 16.augustā

1. LIETOTO TERMINU DEFINĪCIJAS

	LSF Biedrība "Latvijas Slēpošanas federācija", reģistrācijas Nr.40008023069, Grostonas iela 6b, Rīga, Latvija, LV-1013
Tiešais vadītājs	LSF nozīmēts Darbinieka tiešais vadītājs.
	Darbinieks Fiziska persona, LSF darbinieks uz darba vai uzņēmuma līguma pamata, kā arī persona, kas sniedz palīdzību brīvprātīgi.
Vadība	LSF Valde
Politika	Šī Informācijas drošības politika.
	Trešā puse Fiziska persona, juridiska persona vai cita persona, kas nav saistīta ar LSF.

2. MĒRĶIS UN APJOMS

2.1. LSF ir patstāvīga biedrība Latvijas Republikā. LSF biedri ir juridiskas personas, kuru darbība ir saistīta ar slēpošanas sporta un snovborda veidiem, kas veicina slēpošanas, snovborda, tajā skaitā Starptautiskā Slēpošanas federācijā (FIS) atzīto sporta veidu attīstību. LSF saskaņā ar Sporta likumu ir tiesības vadīt un koordinēt darbu slēpošanas sporta veidos valstī, kā arī pārstāvēt valsti attiecīgajā starptautiskajā sporta organizācijā - Starptautiskās Slēpošanas federācijā (FIS).

2.2. Izpildot Sporta likumā noteiktos pienākumus LSF apkopo, uzkrāj, analizē un publisko slēpošanas sporta veidu sacensību dalībnieku datus. Datu apstrāde nepieciešama, lai izpildītu sabiedrības interesēs īstenojamu uzdevumu vai īstenotu oficiālas pilnvaras, kas noteiktas Sporta likumā.

2.3. LSF informācijas drošības sistēmas mērķis ir pasargāt slēpošanas sporta sportistus, LSF 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.

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

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

2.6. Politika var būt piemērojama kopā ar jebkādām citām politikām, noteikumiem, procedūrām un/vai vadlīnijām, ko periodiski pieņem un ievieš LSF.

2.7. Ar visiem informācijas drošības sistēmas jautājumiem un informācijas/datu drošības jautājumiem, kas nav atrunāti šajā Politikā, jāvēršas pie LSF Atbildīgā sekretāra Agra Rauguļa.

3. INFORMĀCIJAS KLASIFIKĀCIJA

3.1. Jebkādu informāciju/datus, kas kļūst pieejami Darbiniekiem, veicot savus darba pienākumus, ja šāda informācija/dati ir saistīti ar LSF un tā darbību, klientiem vai

sadarbības partneriem, uzskata par LSF piederošu un konfidenciālu informāciju, ko, līdz ar to, aizsargā atbilstoši piemērojamie normatīvie akti par konfidenciālas informācijas, tirdzniecības/komercnoslēpumu un personas datu aizsardzību. Šis nosacījums neattiecas uz informāciju, kas publiskojama atbilstoši Valdes noteiktajam uzdevumam.

3.2. Lai nodrošinātu pienācīgu informācijas un datu aizsardzību, LSF 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. LSF lieto šādu vispārīgu informācijas klasifikāciju:

Kategorija	Apraksts	Piemērojamības apjoms (tostarp, bet ne tikai)
Publiska informācija	Informācija, kuru var apstrādāt un izplatīt LSF iekšienē vai ārpus tā, bez jebkādas negatīvas ietekmes uz LSF, jebkuru no tā partneriem, klientiem un /vai saistītajām pusēm.	(a) Sacensību rezultāti un sportistu sasniegumu dati, tādā apjomā, kā to paredz FIS un LSF, Latvijas Olimpiskā komiteja, Latvijas Sporta Federāciju Padome vai cita nozīmēta organizācija. (b) Publiski finanšu pārskati, kurus sniedz valsts iestādēm; (c) 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 LSF pieņemta regulējuma prasības, var kaitēt LSF, LSF reģistrētu slēpošanas sportistu, un/vai jebkura tā Darbinieka, partnera, klientu interesēm.	(a) Jebkura LSF Darbinieka, struktūrvienības izstrādāti un/vai sagatavoti dokumenti, pirms to apstiprināšana LSF Valdē, ja tie nav izstrādāti ar atbilstošu pilnvarojumu; (b) Jebkādi LSF darbības mērķiem izveidoti un/vai lietoti katalogi (kontaktu, informācijas, u. tml.); (c) Jebkādi iekšēji dienesta ziņojumi, paziņojumi, izziņas, slēdzieni, kas izstrādāti LSF darbības vajadzībām.
Iekšējā informācija	Jebkāda informācija, kas ir tik būtiska LSF, jebkuram no tā klientiem un/vai partneriem vai saistītajām pusēm, kuras neautorizēta izpaušana var negatīvi ietekmēt LSF, tā biedru, klientu un/vai sadarbības partneru darbību, operācijas, reputāciju, statusu kopumā, un šādas izpaušanas rezultātā jebkurai no šīm personām var tikt nodarīts nopietns kaitējums.	(a) Politikas, procedūras, iekšējie noteikumi, vadības lēmumi, kas nav paredzēti publiskošanai; (b) Informācija, kas Darbiniekam norādīta kā LSF komercnoslēpums; (c) Cita finanšu, cilvēkresursu, juridiskas, mārketinga dabas informācija, pārdošanas procedūras, plāni un operācijas; (d) Darbības, produkcijas plāni; (e) Personas identifikācijas dati; (f) Informācija, ko aizsargā Darbinieka parakstīta konfidencialitātes vienošanās; (g) Informācija, ko aizsargā konfidencialitātes vienošanās vai sadarbības līgumi, ko LSF ir noslēdzis savas darbības 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 LSD darbībā, uzskatāmi par LSF īpašumu.

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

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 LSF mērķu izpildei un 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 LSF ieskatiem, Darbiniekam var piemērot disciplinārsodu vai atlaist Darbinieku no darba. Tas tāpat var izraisīt pārkāpumu pieļāvušā Darbinieka saukšanu pie administratīvās vai kriminālās 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. 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 LSF noteikumiem.

6.3. Darbinieks piekļūst konfidenciālai informācijai /datiem tikai, ja šādas pilnvaras ir paredzētas attiecīgā Darbinieka Darba līgumā, un/vai ja LSF 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 LSF norādītā, drošā vietā ar tādu uzglabāšanas termiņu, kādu paredz piemērojamie likumi un/vai norāda LSF.

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 LSF apstiprinātā mākoņa krātuvē. 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 LSF 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 pienācīgi aizsargātām, lai novērstu neautorizētu piekļuvi.

7.5. LSF lietotajā aprīkojumā un rīkos var instalēt un lietot tikai LSF pieļautas sistēmas un programmatūru. Pirms jebkādas programmatūras lejupielādēšanas vai instalēšanas Darbiniekiem piederošās un lietotās ierīcēs šajā Politikā aprakstītajiem mērķiem, ir jāsaņem LSF Atbildīgās personas atļauja.

7.6. Gadījumos, kad Darbinieki lieto personīgās (mājas) ierīces, lai piekļūtu LSF 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 LSF nodrošināto aprīkojumu. Līdz ar to, ierīcē ir aizliegts glabāt jebkādus ar LSF saistītus datus un informāciju; jebkāda datu apstrāde ir pieļaujam tikai ar LSF 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 piekrišanu šādai darbībai.

7.8. Gadījumā, ja Darbiniekam tiek piešķirtas tiesības piekļūt LSF 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 LSF ieskatiem, aizsargātie dati/informācija vairs nav nepieciešama LSF mērķu izpildei un 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 LSF informāciju/datus, kas viņiem vairs nav nepieciešami savu darba pienākumu veikšanai, un, jo īpaši, atdot atpakaļ LSF, 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. LSF uzrauga informācijas/datu apstrādē pielietotās sistēmas, lai kontrolētu nepārtrauktu atbilstību šai Politikai un piemērojamajām normatīvajām prasībām.

8. AIZLIEGTĀS DARBĪBAS

8.1. Izņemot īpaši paredzētus izņēmumus, nekādu LSF, tā klientiem vai sadarbības partneriem piederošu aprīkojumu, sistēmas vai rīkus nekādā gadījumā un nekādos apstākļos nedrīkst izmantot ar Darbinieka darba pienākumiem vai ar LSF 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 LSF nav licencēts lietot, uzstādīšana, kopēšana, izplatīšana vai uzglabāšana jebkādās LSF sistēmās vai aprīkojumā, izņemot, brīvā koda programmatūru;

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 LSF darbību vai attiecīgā Darbinieka darba pienākumu veikšanu;

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

f) Jebkādu datu vai informācijas, kurai ir īpašuma un/vai konfidenciāla vērtība LSF, eksportēšana, ja šāda eksportēšana nav nepieciešama LSF komercdarbības vai Darbinieka darba pienākumu veikšanas gaitā, un/vai, ja tā pārkāpj LSF 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 LSF 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 LSF 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.

Apstiprināta ar 2018.gada 16.augusta Biedrības "Latvijas Slēpošanas federācija", reģistrācijas Nr.40008023069, Valdes lēmumu.

Vairis Brīze, LSF prezidents