A P S T I P R I N U
AS „Rīgas Aeronavigācijas Institūts”
Viceprezidents
___ M.Karoļs
“ ___ “ _____2018.g.

A P S T I P R I N U
AS „Rīgas Aeronavigācijas Institūts”
Rektors
_____A.Melnis
“ ___“ _____2018.g.

RĪGAS AERONAVIGĀCIJAS INSTITŪTS
INFORMĀCIJAS DROŠĪBAS POLITIKA

Rīgā, 2018.gada 27. augustā
Vieta, datums

Saturs

1. Lietoto terminu definīcijas

Uzņēmums	***AS “Rīgas Aeronavigācijas Institūts” (turpmāk – RAI)***, reģistrācijas Nr. ***40003083288***, juridiskā adrese ***Mežkalna iela 9, Rīga, LV-1058***, ***Latvija,*** kas ir darba devējs ikvienam darbiniekam, kurš ir nodarbināts uz Darba līguma pamata.
Vadība/ Tiešais vadītājs	Valde un/vai jebkura cita persona Uzņēmumā, kurai piešķirtas vadības funkcijas un pilnvaras.
RAI pārstāvis *(informācijas drošības politikas jomā)*	Sekretariāta vadītāja vai cits Darbinieks, kurš ir iecelts un apstiprināts pārstāvja lomā ar Uzņēmuma rīkojumu.
Darbinieks	Uzņēmuma nodarbināta fiziska persona.
Vadība	Valde un/vai jebkura cita persona Uzņēmumā, kurai piešķirtas vadības funkcijas un pilnvaras.
Trešā puse	Fiziska persona, juridiska persona vai cita persona, kas nav saistīta ar Uzņēmumu.

2. Mērķis un apjoms

2.1. RAI informācijas drošības sistēmas mērķis ir pasargāt RAI 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. Informācijas drošības politika (turpmāk – politika) regulē informācijas apstrādi jebkādās sistēmās vai jebkādos nesējos, kas iesaistīti datu/informācijas apstrādē RAI, neatkarīgi no tā, vai datu/informācijas apstrāde ir saistīta ar RAI iekšējām komercdarbības operācijām vai ārējām attiecībām ar jebkādām trešajām pusēm.

2.3. Šī Politika regulē arī to, kā RAI 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, iekšējās un darba kārtības noteikumiem, RAI Satversmi u. tml. ko periodiski pieņem un ievieš RAI.

2.5. Ar visiem informācijas drošības sistēmas jautājumiem un informācijas/datu drošības jautājumiem, kas nav atrunāti šajā Politikā, jāvēršas pie Vadības un/vai pie sekretariāta vadītājas.

3. Informācijas klasifikācija

3.1. Jebkādu informāciju/datus, kas kļūst pieejami Darbiniekiem, veicot savus darba pienākumus, ja šāda informācija/dati ir saistīti ar RAI un tā darbību, klientiem vai sadarbības partneriem, uzskata par RAI piederošu un konfidenciālu informāciju, kuru 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, RAI 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. RAI lieto šādu vispārīgu informācijas klasifikāciju:

Kategorija	**Apraksts**	**Piemērojamības apjoms (tostarp, bet ne tikai)**
Publiska informācija	Informācija, kuru var apstrādāt un izplatīt RAI iekšienē vai ārpus tā bez jebkādas negatīvas ietekmes uz RAI, 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 RAI pieņemta regulējuma prasības, var kaitēt RAI un/vai jebkura tā	(a) Jebkura RAI Darbinieka, struktūrvienības izstrādāti un/vai sagatavoti dokumenti; (b) Jebkādi RAI komercdarbības mērķiem izveidoti un/vai lietoti katalogi (kontaktu, informācijas, WinStudent datu bāze, Grāmatvedības

	Darbinieka, partnera, klientu interesēm.	datubāzes u. tml.); (c) Jebkādi iekšējie dienesta ziņojumi, paziņojumi, izziņas, slēdzieni, kas izstrādāti RAI komercdarbības vajadzībām.
Konfidenciāla informācija	Jebkāda informācija, kas ir tik būtiska RAI , jebkuram no tā klientiem un/vai partneriem vai saistītajām pusēm, kuras neautorizēta izpaušana var negatīvi ietekmēt RAItā 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 RAI 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 sadarbības līgumi, ko RAI 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 RAI darbībā, uzskatāmi par RAI īpašumu.

4.2. Ikvienam Darbiniekam ir pienākums lietot šādu tehnisko aprīkojumu un rīkus ar pienācīgu rūpību un uzmanību, un tikai ar RAI komercdarbību saistītiem mērķiem. Vienīgais izņēmums ir gadījumi, kad RAI 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 neizpaužnekādām 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 RAI 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 RAI noteikumiem.

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

7.2. Darbiniekiem aizliegts glabāt jebkādu konfidenciālu informāciju savās personīgajās ierīcēs, izņemot informāciju, kas ir īslaicīgi nepieciešama konkrētai, ar darbu saistītai darbībai. Visa nepieciešamā konfidenciālā un personīgi identificējamā informācija jāuzglabā tikai RAI IT personāla apstiprinātā mākoņa krātuvē un RAI 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 RAI 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 RAI IT personāla puses un pienācīgi aizsargātām, lai novērstu neautorizētu piekļuvi.

7.5. RAI lietotajā aprīkojumā un rīkos var instalēt un lietot tikai RAI 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 RAI korporatīvajiem resursiem (piemēram, elektroniskais pasts, tiešsaistes/mākoņa datubāzes), Darbiniekiem ir pienākums ievērot šīs Politikas prasības tieši tāpat kā, ja viņi lietotu RAI nodrošināto aprīkojumu. Līdz ar to ierīcē ir aizliegts glabāt jebkādus ar RAI saistītus datus un informāciju.

Jebkāda datu apstrāde ir pieļaujam tikai ar RAI 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 RAI 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 RAI ieskatiem aizsargātie dati/informācija vairs nav nepieciešami RAI darbībai, šādus datus/informāciju dzēš, iznīcina visas to kopijas, un attiecīgās informācijas /datu apstrādē iesaistītos Darbiniekus attiecīgi informē par viņu pienākumu dzēst/iznīcināt un nodot atpakaļ RAI informāciju/datus, kas viņiem vairs nav nepieciešami savu darba pienākumu veikšanai, un, jo īpaši, atdot atpakaļ RAI, 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.

8. Aizliegtās darbības

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

8.2. Turpmāk minētās darbības ir stingri aizliegtas bez izņēmumiem:

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

(f) Jebkādu datu vai informācijas, kurai ir īpašuma un/vai konfidenciāla vērtība RAI, eksportēšana, ja šāda eksportēšana nav nepieciešama RAI komercdarbības vai Darbinieka darba pienākumu veikšanas gaitā, un/vai, ja tā pārkāpj RAI iekšējos noteikumus, piemērojamos normatīvos aktus;

(g) Darbinieka paroles atklāšana citām personām un citu personu pielaišana lietot to;

(h) Krāpniecisku produkcijas, preču vai pakalpojumu piedāvājumu izveide, izmantojot RAI 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 RAI 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.

Izstrādātājs:

_____

Marina Romele
Sekretariāta vadītāja

PIEŅEMTI:

RAI
Konventa sēdē
2018. g. "07". septembrī
Protokols Nr.1809