INFORMĀCIJAS DROŠĪBAS NOTEIKUMI

(pieaicinātie speciālisti un ārštata pasniedzēji)
(RISEBA informācijas drošības politikas 1.pielikums)

APSTIPRINĀTA
30.augustā, 2022

RISEBA rektora v.i.:
Sagatavoja:
Informācijas tehnoloģiju nodaļas vadītājs
Datu aizsardzības speciālists

Saturs

1. DEFINĪCIJAS

RISEBA	SIA "Biznesa, mākslas un tehnoloģiju augstskola "RISEBA"" (reģ.Nr.40003090010), tās struktūrvienības, filiāles, pārstāvniecības, saistītie uzņēmumi, biedrības.
Vadība	RISEBA rektore; Studiju prorektors; Zinātņu prorektors; Attīstības prorektors; Finanšu direktors; Administratīvais direktors
DAS	RISEBA datu aizsardzības speciālists, dpo@riseba.lv
Resursa turētājs	RISEBA IT nodaļa
Noteikumi	Šie RISEBA Informācijas drošības noteikumi
Trešā persona	Fiziska persona, juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus.
Sadarbības partneri	Piegādātāji, klienti, studenti, pieaicinātie speciālisti, ārštata mācībspēki, pakalpojumu sniedzēji, utt.
RISEBA konts	Jebkurš Lietotājam piešķirtais konts, kuru uztur RISEBA un piekļuve kuram tiek piešķirta personai, stājoties līguma attiecībās ar RISEBA. Piemērs: e-pasts, Sharepoint, MyRiseba, eRiseba, u.tml.
Informācija	Dati, t.sk. personas dati, kas ir RISEBA rīcībā, kas iekļauj, bet neierobežojas ar konfidenciālo, ierobežotas pieejamības, iekšējās lietošanas informāciju.
RISEBA ierīces	Visas informācijas un datu apstrādei, glabāšanai un pārraidei paredzētas ierīces (ieskaitot galda datorus, klēpjdatorus, planšetdatorus, viedtālruņus un citas rokas ierīces), kas pieder RISEBA.
RISEBA telpas	Telpas, kuras pieder RISEBA vai kurus RISEBA iznomā, un kurām ir nodrošināta fiziskā aizsardzība un piekļuves kontrole.
RISEBA dati	Jebkuri dati, t.sk. personas dati, kurus iegūst, apstrādā un pārvalda RISEBA, kā arī jauni dati, kuri rodas, apstrādājot un izmantojot šos datus.
Lietotājs	Persona, kurai ir izveidots RISEBA konts un ir piešķirta piekļuve RISEBA informācijai (piem., pieaicināties speciālisti, ārštata pasniedzēji).

2. NOTEIKUMU MĒRĶIS UN APRAKSTS

2.1. Noteikumu mērķis ir nodrošināt RISEBA informācijas sistēmu pārvaldības ieviešanu un uzturēšanu, kas nodrošina nepārtrauktu RISEBA informācijas sistēmu drošību un aizsargā RISEBA informācijas aktīvus no nepilnvarotas piekļuves un to ļaunprātīgas izmantošanas.

2.2. Noteikumi attiecas uz informācijas un datu apstrādi jebkurās sistēmās un izmantojot jebkurus datu nesējus, kas iesaistīti datu/informācijas apstrādē, neatkarīgi no tā, vai datu/informācijas apstrāde notiek attiecību ar RISEBA ietvaros vai attiecībās ar Trešajām personām.

2.3. Noteikumi nosaka arī to, kā RISEBA Lietotāji izmanto aprīkojumu un rīkus, kas viņiem ir pieejami, lai veiktu savus līguma pienākumus.

2.4. Noteikumi var būt piemērojami kopā ar visām citām politikām, noteikumiem, rīkojumiem un vadlīnijām, kuras pieņem un ievieš RISEBA.

2.5. Visus informācijas drošības sistēmas un informācijas drošības jautājumus, kuri nav atspoguļoti šajos Noteikumos, ir jāadresē Resursa turētājam un DAS.

2.6. Lietotājiem ir pienākums ievērot Noteikumus, kā arī piemērojamo Latvijas vai starptautisko normatīvo aktu prasības, kas nosaka informācijas apstrādes un aizsardzības noteikumus.

3. PERSONAS DATU AIZSARDZĪBA

3.1. Visi personas dati un cita informācija, ar kuras palīdzību var identificēt datu subjektus, var tikt apkopoti un apstrādāti tikai, ja pastāv šādu personas datu apstrādes juridiskais pamats un ciktāl tas nepieciešams Lietotāja līgumisko pienākumu

veikšanai, ar nosacījumu, ka šādas darbības tiek veiktas Lietotājam piešķirto pilnvaru ietvaros un saskaņā ar likumā noteiktajām datu aizsardzības prasībām.

3.2. Sakarā ar šo, ir strikti jāievēro personas datu apstrādes noteikumi, kuri Lietotājiem ir darīti zināmi starp RISEBA un Lietotāju noslēgtajā līgumā vai tā pielikumos, un jāīsteno pasākumi, kas jo īpaši atbilst integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principiem.

4. SISTĒMAS, KURAS IZMANTO DATU UN INFORMĀCIJAS APSTRĀDEI

4.1. Jebkuras informācijas sistēmas, ieskaitot, bet neierobežojoties ar datortehniku, jebkura veida programmatūru, mākoņa platformām un pakalpojumiem, operētājsistēmām, jebkuru datu nesēju, tīkla kontiem, elektroniskā pasta kontiem, pārlūkošanas sistēmām un jebkura cita tehniskā bāze un rīki, kas pieder RISEBA, Lietotājam ir jāizmanto ar pienācīgu rūpību un uzmanību un tikai ar RISEBA darbību saistītiem mērķiem.

5. DROŠĪBAS PASĀKUMI, VEICOT DATU UN INFORMĀCIJAS APSTRĀDI

5.1. Šie Noteikumi, kā arī normatīvie akti, kas nosaka datu drošības prasības, attiecas uz visām informācijas formām (papīra formātā, elektroniskā veidā utt.) un tās apstrādes veidiem (datu vākšana, apstrāde, aizsardzība, glabāšana, u.c.) un Lietotāji ir atbildīgi par to, ka Lietotāja rīcībā esošie RISEBA dati tiktu droši pārvaldīti, t.sk. ievērojot Vispārīgās datu aizsardzības regulas prasības.

5.2. Lietotājiem ir pienākums vienmēr uzmanīt līgumattiecību pildīšanas vajadzībām izmantotas ierīces un datu nesējus (turpmāk – Ierīces), kā arī glabāt tās drošā vietā. Kad tās netiek izmantotas vai tiek atstātas bez novērošanas, Ierīces ir jāaizsargā ar paroli vai jāizslēdz, bet datu nesēji jāievieto drošā glabātuvē.

5.3. Datiem, kas tiek apstrādāti elektroniskā veidā ārpus RISEBA telpām un kuros nav brīvi pieejama publiska informācija, jānodrošina šifrēšana visos apstrādes posmos.

5.4. Lietotājiem ir aizliegts izmantot citu organizāciju e-pasta kontus ar RISEBA darbību saistītā saziņā, kā arī pārsūtīt jebkuru ar RISEBA darbību saistīto informāciju uz citu organizāciju e-pasta kontiem un / vai mākoņa platformām.

5.5. Kad datu apstrādes turpināšanai nepastāv pietiekamie leģitīmie pamati, it īpaši, ja ar Lietotāju tiek izbeigtas līgumiskas attiecības, Lietotājam RISEBA dati ir jāizdzēš un visas kopijas jāiznīcina. RISEBA var papildus informēt Lietotāju par to, kuri RISEBA dati ir jāiznīcina vai jāatgriež atpakaļ RISEBA.

5.6. Lietotājiem Ir stingri aizliegts lietot interneta publiskos pieslēgumus (piemēram, interneta kafejnīcā, bibliotēkās, kafejnīcā u.tml.) piekļuvei RISEBA datiem, izņemot gadījumus, kad līguma pienākumu izpilde notiek ārpus Latvijas vai tā ir kritiska un neatliekama ar līguma pienākumu saistīta nepieciešamība un Resursa turētājs sniedzis skaidru piekrišanu šādai darbībai. Visos citos gadījumos ir jāizmanto mobilo sakaru tīkls.

5.7. Izmantojot RISEBA ierīces, pārlūkošana Lietotāja privātām vajadzībām ir atļauta, izņemot tiešsaistes spēļu vai azartspēļu spēlēšanai un datu koplietošanu, kā arī vietņu aplūkošanu ar tādu aizliegtu saturu kā pornogrāfija, ieroči, terorisms, ekstrēmisms, un citas negatīva rakstura vietnes. Īstenojot informācijas sistēmu drošības pārvaldību, RISEBA var analizēt interneta datu plūsmu, lai konstatētu uzbrukumus tīklam.

6. PIEKĻUVES PĀRVALDĪBA

6.1. Jebkuras Lietotājiem pieejamās piekļuves tiesības tiek piešķirtas, ņemot vērā līguma pienākumus un pamatojoties uz "nepieciešamību zināt" principu. Piekļuve jebkurai RISEBA sistēmai nenozīmē, ka Lietotājs ir pilnvarots izmantot visu informāciju, ko satur šāda sistēma.

6.2. Saņemot piekļuves datus RISEBA sistēmām (lietotāja vārdu un pagaidu paroli), Lietotājam ir pienākums nekavējoties nomainīt paroli pēc pirmās pieslēgšanās sistēmai.

6.3. Lietotāju piekļuves dati sistēmām ir unikāli un identificē konkrētu Lietotāju. Katrs Lietotājs ir atbildīgs par visām darbībām, kas saistītas ar viņu personas identifikācijas kontiem, tāpēc viņu galvenais pienākums ir nodrošināt, lai piekļuves dati nebūtu pieejami nevienai Trešajai personai vai citām personām, izņemot gadījumus, kad RISEBA norādīja citādi.

6.4. Sistēmas drošības paroļu prasības:

6.4.1. Lietotājam ir jāizmanto paroles, kuras nav viegli uzminamas:
- paroles nedrīkst ietvert Lietotāja personas datus;
- minimālais rakstzīmju skaits - 8, minimālais lielo burtu skaits - 1, minimālais speciālo simbolu skaits – 1;
- paroli nedrīkst izmantot atkārtoti.

6.5. Ja maksimālais nesekmīgo piekļuves mēģinājumu skaits pārsniedz 5 reizes vienā kalendārā dienā, piekļuve kontam tikts slēgta automātiski. Tiesības atbloķēt kontu ir tikai Resursa turētājam. Minēto kontroli piemēro neatkarīgi no tā, vai piekļuves mēģinājums tiek veikts lokālajā datu pārraides tīklā vai publiskajā datu pārraides tīklā.

6.6. Katrs Lietotājs ir personīgi atbildīgs par savu drošības paroļu atbilstību šiem Noteikumiem un visiem citiem RISEBA piekļuves datu drošības noteikumiem, ja tādi ir darīti zināmi Lietotājam.

7. RISEBA UN PERSONISKO IERĪČU IZMANTOŠANA. ATTĀLINĀTAIS DARBS.

7.1. Veicot līguma pienākumus RISEBA telpās, datu apstrādei Lietotājam ir jāizmanto RISEBA ierīces. Parasti tādas ierīces iekļauj, bet neierobežojas ar stacionāro datoru un/vai klēpjdatoru, ar kuru Lietotājs var pieslēgties RISEBA serveriem un tīklam. Kad RISEBA ierīču izmantošana būtiski traucē, kavē vai padara neiespējamu līguma pienākumu sniegšanu katrā konkrētajā gadījumā, kā arī gadījumos, kad Lietotājs strādā attālināti, Lietotājam ir atļauts izmantot personīgas ierīces. Izmantojot personīgas ierīces, Lietotājiem ir jāievēro šo Noteikumu 5., 7.2. un 7.3.punktu prasības.

7.2. Ierīcēm, ko Lietotāji izmanto līguma pienākumus pildīšanai, jāatbilst sekojošiem prasījumiem:

7.2.1. Uz ierīcēm ir atļauts instalēt un izmantot tikai licencētas un atļautas programmatūras;

7.2.2. Uz ierīcēm instalētai programmatūrai jābūt regulāri atjaunotai, lai novērstu kļūmes un ievainojumus;

7.2.3. Ja ierīce ir viedtālrunis vai planšetdators / klēpjdators:

- Ierīcei ir jābūt paroles (vai līdzvērtīgas) bloķēšanas funkcionalitātei;
- Parolei (vai līdzvērtīgam risinājumam) jābūt vienmēr iespējotai;
- Planšetdatoram ir jābūt iespējotai un aktuālai vīrusu un ļaunprātīgas programmatūras aizsardzībai. Ja ir iespējams, minētais nosacījums ir jāīsteno arī attiecībā uz viedtālruni;
- Ierīcei jābūt ieslēgtai attālinātās atrašanās vietas noteikšanas funkcijai;
- Dati un informācija jāglabā šifrētā veidā.

7.2.4. Ja ierīce ir stacionārais dators:

- Piekļuvei ierīcei jābūt bloķētai ar paroli (vai līdzvērtīgo risinājumu);
- Parolei (vai līdzvērtīgam risinājumam) jābūt vienmēr iespējotai;
- Ierīcei jābūt aktuālai aizsardzībai pret vīrusiem un ļaunprātīgu programmatūru;

7.2.5. Ja ierīce ir jebkura cita ierīce:

- Piekļuvei ierīcei jābūt bloķētai ar paroli (vai līdzvērtīgo risinājumu);
- Dati un informācija jāglabā šifrētā veidā. Ja ierīce nav spējīga šifrēt, tādā gadījumā informācija jāšifrē pirms tās pārsūtīšanas uz ierīci.

7.3. Citām organizācijām piederošo ierīču izmantošana nav atļauta.

7.4. Ja Lietotāja ierīce paredz tādu iespēju, visi RISEBA dati jāglabā atsevišķi no citiem datiem, mapē ar individuālu šifrēšanas iespēju un/vai individuālu paroles aizsardzību. Lietotājam ir jāizdzēš RISEBA dati no ierīces, kad to glabāšana vairs nav nepieciešama konkrētā darba uzdevuma vai līguma pienākuma izpildei.

7.5. Ja Lietotājs saņem paziņojumu par to, ka viņa izmantotajā ierīcē ir atrasts vīruss, ir stingri aizliegts piekļūt jebkuram ierīces failam, kas satur RISEBA datus, kā arī jāaizver jebkuru atvērtu logu vai paziņojuma logu un nekavējoties jāsazinās ar Resursa turētāju un jāinformē par notikušo.

7.6. Par personīgās ierīces, kurā tika glabāti un apstrādāti RISEBA dati, nozaudēšanu, nekavējoties jāinformē Resursa turētājs un DAS.

8. DATU NESĒJU GLABĀŠANAS UN IZNĪCINĀŠANAS KĀRTĪBA

8.1. Lietotājam ir aizliegts izmantot citai organizācijai piederošus elektroniskus datu nesējus RISEBA datu glabāšanai vai pārsūtīšanai (piemēram, atmiņas kartes, ārējie/noņemamie diskdziņi, zibatmiņas/USB diski, kompaktdiski).

8.2. RISEBA datus, kuri ir klasificēti ka konfidenciālie vai ierobežotas piekļuves dati, ir atļauts glabāt tikai uz tādiem elektroniskiem nesējiem, kuriem ir iespējota paroļu aizsardzība un datu šifrēšana.

8.3. Kad informācija, ko satur RISEBA datu nesēji, vairs nav nepieciešama, informācijai jābūt izdzēstai no elektroniskā datu nesēja nekavējoties.

8.4. Darbam ar RISEBA datiem ir aizliegts izmantot elektroniskus datu nesējus, kuri ir salauzti vai nepilda savu funkciju pilnvērtīgi.

8.5. Ir aizliegta jebkuras citas personas piekļuve elektroniskiem datu nesējiem, kurā Lietotājs glabā RISEBA datus,

8.6. Ja datu nesēji tiek nodoti lietošanai citām personām, Lietotājs, kas nodod datu nesēju, pārliecinās, ka tas nesatur RISEBA datus un nodod to citas personas lietošanā tikai pēc tajā esošo datu dzēšanas.

9. AIZLIEGTĀS DARBĪBAS

9.1. Izņemot gadījumus, kad to atļauj RISEBA, nekādā gadījumā iekārtas, sistēmas vai rīkus, kas pieder RISEBA vai Sadarbības partneriem, nedrīkst izmantot mērķiem, kas nav saistīti ar Lietotāja līgumiskiem pienākumiem vai nav saistīti ar RISEBA darbību.

9.2. Ir stingri aizliegts veikt šādas darbības:

(a) Jebkuras personas vai uzņēmuma tiesību, kas aizsargāti ar intelektuālā īpašuma tiesībām, pārkāpšana, ieskaitot, bet neierobežojoties ar jebkuras nelegālas programmatūras, tiešsaistes platformu, jebkura cita elektroniska satura, kas ar noteikto līgumu nav piešķīris RISEBA tā lietošanas licenci, instalēšanu, kopēšanu, izplatīšanu vai glabāšanu jebkurās RISEBA sistēmās vai aprīkojumā;
(b) Autortiesību aizsardzības objektu neatļauta kopēšana;
(c) Jebkura datu subjekta tiesību pārkāpums, pārmērīgi un bez noteiktā pamata vācot un apstrādājot šāda datu subjekta personas datus;
(d) Piekļuve datiem, serverim vai kontam ar nolūku, kas nav saistīts ar RISEBA darbības veikšanu vai Lietotāja līgumisku pienākumu veikšanu;
(e) Programmatūras, tehniskās informācijas, šifrēšanas programmatūras vai tehnoloģijas eksportēšana, pārkāpjot piemērojamos starptautiskos vai nacionālos likumus un noteikumus un / vai RISEBA norādījumus;
(f) Lietotāja piekļuves datu RISEBA sistēmām atklāšana un iespējas nodrošināšana citām personām lietot personīgo kontu (ieskaitot, bet neierobežojoties ar Lietotāja ģimenes locekļiem);
(g) Piedāvāt krāpnieciskus vai ar privātām interesēm saistītus produktus vai pakalpojumus no RISEBA konta;
(h) Ietekmēt drošības pārkāpumu vai tīkla sakaru pārtraukšanu. Šādi drošības pārkāpumi ietver, bet neaprobežojas ar: piekļuve datiem, kuri nav domāti atklāšanai Lietotājam, vai Lietotāja ielogošanās vai piekļuve serverim vai kontam bez speciālās atļaujas, ja vien šādi pienākumi nav Lietotāja līgumiskie pienākumi vai piekļuves tiesības Lietotājam tiek piešķirtas sakarā ar atsevišķu RISEBA projektu;
(i) Jebkuras programmas / skripta / komandas izmantošana vai jebkura veida ziņojumu sūtīšana, ar mērķi traucēt vai atspējot cita lietotāja sesiju.

10. DROŠĪBAS PĀRKĀPUMU INCIDENTU PAZIŅOŠANA UN APSTRĀDE

10.1. Par visiem datu apstrādes drošības incidentiem vai starpgadījumiem, kas var izraisīt RISEBA datu apstrādes drošības pārkāpumus, Lietotājam nekavējoties jāziņo vienlaicīgi Resursa turētājam un DAS.

10.2. Resursa turētājs un DAS organizē visus nepieciešamus pasākumus, lai novērstu iespējamo pārkāpumu vai zaudējumus, vai mazinātu tā sekas un atjaunotu iepriekšējo drošības stāvokli, nepieciešamības gadījumā piesaistot citus darbiniekus un Vadību.

11. NOSLĒGUMA NOTEIKUMI

11.1. Šie noteikumi ir neatņemama RISEBA Informācijas drošības politikas sastāvdaļa. Ja normatīvie akti nenosaka citādi, Lietotāji tiek iepazīstināti ar šiem Noteikumiem elektroniski vai papīra formā, un tiks uzskatīts, ka Noteikumi kļuva pieejami Lietotājam, Lietotājs ar tiem ir iepazinies un Noteikumi kļūst saistoši to saņemšanas dienā (attiecīgā e-pasta saņemšanas, paziņošanas brīdis citā elektroniskajā vidē vai Noteikumu papīra formā nodrošināšanas brīdis).

Dokumenta klasifikācija: RISEBA konfidenciālā informācija					
Nosaukums:	RISEBA informācijas drošības noteikumi (Pielikums Nr.1)				
Atbildīgā persona:	IT nodaļas vadītājs	**Dokumentu apstiprina:**	RISEBA rektora v.i.		
		Dokumentu saskaņo	Datu aizsardzības speciālists		
Statuss:	Spēkā esošs	**Redakcija:**	1.0	**Datums:**	30.08.2022