INFORMĀCIJAS DROŠĪBAS NOTEIKUMI

Studējošie

(RISEBA informācijas drošības politikas 2.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.
DAS	RISEBA datu aizsardzības speciālists, dpo@riseba.lv
Resursa turētājs	RISEBA IT nodaļa
Lietotājs	Studējošais, ar kuru RISEBA ir noslēgts Studiju līgums vai cita veida līgums, pamatojoties uz kuru persona piedalās studijās vai apmācībās, kuras īsteno RISEBA.
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.
Noteikumi	Šie RISEBA Informācijas drošības noteikumi
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 paredzētās ierīces (ieskaitot galda datorus, klēpjdatorus, planšetdatorus)), kas pieder RISEBA.
RISEBA telpas	Telpas, kuras pieder RISEBA vai kuras 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.
Personas dati	jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu. Identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.

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 RISEBA studiju ietvaros vai attiecībās ar Trešajām personām.

2.3. Noteikumi nosaka arī to, kā RISEBA Lietotāji izmanto aprīkojumu un rīkus, kas viņiem ir pieejami, studējot RISEBA.

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. INFORMĀCIJAS APSTRĀDE

3.1. 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.

3.2. Jebkura informācija vai RISEBA dati, kas kļūst pieejami Lietotājiem, studējot RISEBA un izmantojot RISEBA ierīces, tiek uzskatīti par RISEBA informāciju, uz kuru RISEBA ir īpašumtiesības. Tādējādi, šī informācija ir pakļauta īpašai aizsardzībai saskaņā ar šiem Noteikumiem, piemērojamiem normatīvajiem aktiem par konfidenciālas informācijas, komercnoslēpumu un personas datu aizsardzību, un nedrīkst tikt izpausta Trešajām personām, kamēr RISEBA nepaziņo, ka šāda informācija ir kļuvusi publiska vai citādi pārkvalificēta par informāciju, uz kuru vairs neattiecas šo Noteikumu aizsardzības noteikumi.

3.3. RISEBA dati ir pakļauti aizsardzībai neatkarīgi no tā, vai šāda informācija Lietotāja rīcībā ir nonākusi drukātos materiālos, mutiski, datu nesējos vai audio / video materiālos, u.tml.

3.4. Ja Lietotājam nav pārliecības vai pieejamie RISEBA dati ir publiskie dati, ar tiem jārīkojas kā ar konfidenciālo informāciju.

4. DROŠĪBAS PASĀKUMI, VEICOT DATU UN INFORMĀCIJAS APSTRĀDI

4.1. 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.

4.2. Lietotājiem ir pienākums vienmēr uzmanīt studiju vajadzībām izmantotās ierīces (turpmāk – Ierīces), kā arī glabāt tās drošā vietā. Kad tās netiek izmantotas vai tiek atstātas bez novērošanas, Ierīces ir jāaizsargā ar paroli vai jāizslēdz.

4.3. Sakarā ar augstu drošības risku, Lietotājiem ir rekomendējams neizmantot interneta publiskos pieslēgumus (piemēram, interneta kafejnīcā, bibliotēkās, kafejnīcā u.tml.) piekļuvei RISEBA kontiem un iespēju robežās jācenšas izmantot ierīces mobilo sakaru tīkls.

4.4. 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.

5. PIEKĻUVES PĀRVALDĪBA

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

5.2. 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, kā arī citām personām, izņemot gadījumus, kad RISEBA norādīja citādi.

5.3. Sistēmas drošības paroļu prasības:

5.3.1. 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.

5.4. Ja maksimālais nesekmīgo piekļuves mēģinājumu skaits pārsniedz 5 reizes vienā kalendārā dienā, piekļuve kontam tikts slēgta automātiski. Tiesības atbloķēt kontu ir tikai Resursa turētājam.

5.5. 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.

6. PERSONISKO IERĪČU IZMANTOŠANA.

6.1. Ierīcēm, ko Lietotāji izmanto, lai pieslēgtos RISEBA kontiem, jāatbilst sekojošiem prasījumiem:

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

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

6.1.3. Ierīcei ir jābūt paroles (vai līdzvērtīgas) bloķēšanas funkcionalitātei;

6.1.4. Parolei (vai līdzvērtīgam risinājumam) jābūt vienmēr iespējotai;

6.1.5. Ierīcei ir jābūt iespējotai un aktuālai vīrusu un ļaunprātīgas programmatūras aizsardzībai.

6.2. Citām organizācijām piederošo ierīču izmantošana nav atļauta.

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

7. AIZLIEGTĀS DARBĪBAS

7.1. Ir stingri aizliegts veikt šādas darbības:

(a) Pārkāpt jebkuras personas vai uzņēmuma tiesības, kas aizsargātas ar intelektuālā īpašuma tiesībām, 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 RISEBA ierīcēs;
(b) Bez atļaujas kopēt autortiesību aizsardzības objektus;
(c) pārkāpt datu subjekta tiesības, pārmērīgi un bez noteikta pamata vācot un apstrādājot šāda datu subjekta personas datus;
(d) piekļūt RISEBA kontam ar nolūku, kas nav saistīts ar studijām vai citiem no studiju līguma izrietošām saistībām;
(e) Eksportēt programmatūru, tehnisko informāciju, šifrēšanas programmatūru vai tehnoloģiju, pārkāpjot piemērojamos starptautiskos vai nacionālos likumus un noteikumus un / vai RISEBA norādījumus;
(f) Atklāt Lietotāja piekļuves datus RISEBA kontiem un sistēmām un iespējas nodrošināšana citām personām lietot personīgo RISEBA 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 piekļuves tiesības Lietotājam tiek piešķirtas sakarā ar atsevišķu RISEBA projektu;
(i) Izmantot jebkuras programmas / skriptus / komandas vai sūtīt jebkura veida ziņojumus ar mērķi traucēt vai atspējot cita lietotāja sesiju.

8. DROŠĪBAS PĀRKĀPUMU INCIDENTU PAZIŅOŠANA UN APSTRĀDE

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

9. NOSLĒGUMA NOTEIKUMI

9.1. 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.2)				
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