INFORMĀCIJAS DROŠĪBAS POLITIKA

(darbinieki)

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 rektors; Studiju prorektors; Zinātņu prorektors; Attīstības prorektors; Finanšu direktors; Administratīvais direktors
Tiešais vadītājs	RISEBA pārstāvis, Darbinieks, kurš ir norādīts attiecīgā darbinieka darba līgumā vai iecelts ar RISEBA rīkojumu kā tiešais darbinieka un/vai nodaļas vadītājs.
Darbinieks	Jebkura persona, ar kuru RISEBA ir darba tiesiskās attiecības.
DAS	RISEBA datu aizsardzības speciālists, dpo@riseba.lv
Resursa turētājs	RISEBA IT nodaļa
Politika	Šī RISEBA informācijas drošības politika
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 Darbiniekam piešķirtais konts, kuru uztur RISEBA un piekļuve kuram tiek piešķirta Darbiniekam, stājoties darba tiesiskajās 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, kuri pieder RISEBA vai kurus RISEBA iznomā, un kurām ir nodrošināta fiziskā aizsardzība un piekļuves kontrole.
Lietotājs	Persona, kurai ir izveidots RISEBA konts un ir piešķirta piekļuve RISEBA informācijai.

2. POLITIKAS MĒRĶIS UN APRAKSTS

2.1. Informācijas drošības politikas 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 tās ļaunprātīgas izmantošanas.

2.2. Šī Politika 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 darba tiesisko attiecību ar RISEBA ietvaros vai attiecībās ar Trešajām personām.

2.3. Šī politika nosaka arī to, kā RISEBA darbinieki izmanto aprīkojumu un rīkus, kas viņiem ir pieejami, lai veiktu savus darba pienākumus.

2.4. Politika var būt piemērojama 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 šajā Politikā, ir jāadresē Resursa turētājam un DAS.

2.6. Darbiniekiem ir pienākums ievērot Politiku, kā arī piemērojamo Latvijas vai starptautisko normatīvo aktu prasības, kas nosaka informācijas apstrādes un aizsardzības noteikumus. Politikas noteikumu un citu datu aizsardzības noteikumu neievērošana tiek uzskatīta par būtisku darba kārtības pārkāpumu un pēc RISEBA ieskatiem var būt pamats disciplinārsodu piemērošanai vai Darbinieka atlaišanai, kā arī tai var sekot administratīvā vai krimināltiesiskā atbildība.

3. PERSONAS DATU AIZSARDZĪBA

3.1. Visi personas dati un cita informācija, ar kuras palīdzību var identificēt datu subjektus, tiek apkopoti un apstrādāti tikai, ja pastāv šādu personas datu apstrādes juridiskais pamats un ciktāl tas nepieciešams Darbinieka darba pienākumu veikšanai, ar nosacījumu, ka šādas darbības tiek veiktas Darbiniekam piešķirto pilnvaru ietvaros un saskaņā ar likumā noteiktajām datu aizsardzības prasībām.
3.2. Sakarā ar šo, ir strikti jāievēro iekšējās personas datu apstrādes politikas noteikumi un jāīsteno pasākumi, kas jo īpaši atbilst integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principiem.
3.3. Datu subjektu pieprasījumu un sūdzību apstrādi, kā arī atbilžu sagatavošanu veic RISEBA DAS. Saņemot datu subjekta pieprasījumu vai sūdzību attiecībā uz viņa/-as personas datiem, Darbinieks nekavējoties informē par šādu pieprasījumu DAS, pievienojot situācijas aprakstu, kā arī citu ar konkrētiem personas datiem saistītu informāciju.

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, ko izmanto RISEBA, tiek uzskatīti par RISEBA īpašumu.

4.2. Jebkuram Darbiniekam 4.1.punktā minētais tehniskais aprīkojums un rīki jāizmanto ar pienācīgu rūpību un uzmanību un tikai ar RISEBA darbību saistītiem mērķiem. Vienīgais izņēmums ir gadījumi, kad RISEBA piešķīra Darbiniekam tehnisko aprīkojumu (piemēram, mobilo tālruni) un nepārprotami atļauj to izmantot arī privātiem mērķiem.

4.3. Visām RISEBA izmantotajām sistēmām, programmatūrai un iekārtām jābūt atbilstoši licencētām un likumīgi iegādātām.

4.4. RISEBA regulāri (vismaz reizi kvartālā) pārbauda un atjaunina informācijas / datu apstrādē izmantotās sistēmas un programmatūras, lai nodrošinātu nepārtrauktu visu RISEBA informācijas tehnoloģiju sistēmu drošību un integritāti, kā arī šīs Politikas un piemērojamo likumu prasību pastāvīgu ievērošanu un nodrošināšanu.

4.5. Katrai informācijas sistēmai RISEBA nozīmē sistēmas valdītāju (*system owner*).

4.6. Informācijas sistēmas valdītājs ir atbildīgs par:

- Informācijas sistēmu pieejamību, integritāti un konfidencialitāti;
- Informācijas sistēmu iegādes, izstrādes, modificēšanas un darba procesa koordinēšanu un vadīšanu;
- Informācijas sistēmu ieviešanu un tālāku uzturēšanu;
- Komunikācijas uzturēšanu ar informācijas sistēmu piegādātāju;
- Informācijas sistēmu pieejas tiesību noteikšanu un regulāru pārskatīšanu;
- finansiālu resursu piesaistes procesa organizēšanu un pārraudzību, kuri ir nepieciešami IS ieviešanai un uzturēšanai (piemēram, licenču iegādei vai atjaunošanai, atbalsta iegādei, ārpakalpojuma abonēšanai).

5. DROŠĪBAS PASĀKUMI, VEICOT DATU UN INFORMĀCIJAS APSTRĀDI

5.1. Šī Politika, 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.).

5.2. Darbinieki ir atbildīgi par to, lai Darbinieka rīcībā esošie RISEBA dati tiktu droši pārvaldīti. Visi dati ir jāglabā RISEBA ierīcēs, serveros, kontos vai pieejamajā vidē (piem., Sharepoint, Onedrive, tīkla disks). Lai glabātu RISEBA datus citās glabātuvēs, ir nepieciešama skaidra, rakstiska Resursa turētāja atļauja.

5.3. Darbiniekiem ir pienākums vienmēr uzmanīt darba vajadzībām izmantotās ierīces un datu nesējus, kā arī glabāt tos drošā vietā. Kad ierīces netiek izmantotas vai tiek atstātas bez novērošanas, tās ir jāaizsargā ar paroli vai jāizslēdz, bet datu nesēji jāievieto drošā glabātuvē.

5.4. Datiem, kas tiek apstrādāti elektroniskā veidā ārpus RISEBA telpām vai sadarbības partnera droša datu centra telpām, un kuri nav uzskatāmi par brīvi pieejamo publisko informāciju, jānodrošina šifrēšana visos apstrādes posmos.

5.5. Darbiniekiem ir aizliegts izmantot savus privātos vai citu organizāciju e-pasta kontus ar RISEBA darbību saistītā saziņā, kā arī pārsūtīt jebkuru ar RISEBA darbību saistīto informāciju uz saviem privātajiem vai citu organizāciju e-pasta kontiem un / vai mākoņa platformām, kuras Darbinieks izmanto privāti vai veicot ar RISEBA nesaistītus darbus.

5.6. Kad datu apstrādes turpināšanai nepastāv pietiekamie leģitīmie pamati, datus izdzēš, visas kopijas iznīcina un attiecīgie Darbinieki tiek informēti par to, ka dati, kas atrodas viņu rīcība ir jāiznīcina vai jāatgriež atpakaļ RISEBA, it īpaši, ja ar Darbinieku tiek izbeigtas darba tiesiskās attiecības.

6. PIEKĻUVES PĀRVALDĪBA

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

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

6.3. Ja pieslēgšanās RISEBA informācijas sistēmām notiek ārpus RISEBA telpām un, ja sistēma paredz tādu iespēju, Darbiniekam jāveic autentifikācija elektroniskajā vidē, izmantojot divpakāpju verifikācijas sistēmu.

6.4. Darbinieku piekļuves dati sistēmām ir unikāli un identificē konkrētu Darbinieku. Katrs Darbinieks 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 citiem Darbiniekiem vai personām, izņemot gadījumus, kad RISEBA vai Darbinieka Tiešais vadītājs norādījis citādi.

6.5. Sistēmas drošības paroļu prasības:

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

6.5.2. Resursa turētājam ir jānodrošina:
- lai ne retāk kā reizi 3 mēnešos Darbiniekiem tiktu pieprasīta paroļu nomaiņa sistēmām;
- automātiskās paroles sarežģītības un 6.5.1.punktā noteikto nosacījumu izpildes pārbaude;
- paroļu lielo un mazo burtu jutīgums.

6.6. 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.

6.7. Katrs Darbinieks ir personīgi atbildīgs par savu drošības paroļu atbilstību šai Politikai un visiem citiem RISEBA piekļuves datu drošības noteikumiem.

6.8. Regulāri, bet ne retāk kā reizi gadā, Resursa turētājs pārskata RISEBA informācijas sistēmu lietotāju tiesības, kā arī katru reizi, kad:
- tiek izbeigtas darba tiesiskās attiecības ar Darbinieku, Resursa turētājs anulē šī Lietotāja piekļuves tiesības RISEBA informācijas sistēmām. Anulējot Darbinieka lietotāju tiesības, Resursa turētājs nodrošina Darbinieka vadītājam piekļuvi Darbinieka e-pastam, ko iepriekš pārvaldīja šīs Darbinieks.
- gadījumos, ka Darbinieki tiek norīkoti vai pārcelti citos amatos.

7. RISEBA UN PERSONISKO IERĪČU IZMANTOŠANA. ATTĀLINĀTAIS DARBS.

7.1. Veicot darba pienākumus RISEBA telpās, datu apstrādei Darbiniekam jāizmanto RISEBA ierīces. Parasti tādas ierīces iekļauj, bet neierobežojas ar stacionāro datoru, klēpjdatoru, viedtālruni vai planšetdatoru, ar kuru Darbinieks var pieslēgties RISEBA serveriem un tīklam. Gadījumos, kad Darbinieks strādā attālināti, darbam ar RISEBA datiem Darbiniekiem ir atļauts izmantot personīgas ierīces tikai, ja tiek ievērotas šīs Politikas 7.3. un 7.4.punktu prasības.

7.2. Ja attālinātā darba īstenošanai RISEBA ierīču piešķiršanu pieprasa vairāki Darbinieki, taču Resursa turētāja rīcībā nav pietiekama ierīču skaita, priekšroka tiek dota administratīvā personāla Darbiniekam, kura darbs paredz lielāku apstrādājamo datu apjomu, un tikai pēc tam akadēmiskā personāla Darbiniekam.

7.3. RISEBA ierīcēm, ko Darbinieki izmanto darba vajadzībām, jāatbilst sekojošiem prasījumiem:

7.3.1. Uz ierīcēm ir atļauts instalēt un izmantot tikai licencētas un atļautas programmatūras, kuru nepieciešamību izvērtē un apstiprina Resursa turētājs pirms programmatūras lejupielādes vai instalēšanas ierīcēs.

7.3.2. Uz ierīcēm instalētai programmatūrai jābūt regulāri atjaunotai, lai novērstu kļūmes un ievainojumus. Ja programmatūras izstrādātājs vairs nenodrošina to atbalstu, programmatūras izmantošana nav atļauta bez riska izvērtēšanas, ko veic Resursa turētājs kopā ar DAS, izstrādājot nepieciešamo dokumentāciju.

7.3.3. 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.

7.3.4. 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.

7.3.5. 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.

7.4. Visas Ierīces, kuras Darbinieks izmanto RISEBA informācijas apstrādei un kuras nav RISEBA īpašums, jāapstiprina Resursa turētājam. Citām organizācijām piederošo ierīču izmantošana nav atļauta.

7.5. Gadījumos, kad Darbinieks izmanto personīgās ierīces, lai piekļūtu RISEBA serveriem un tīklam, Darbiniekam ir pienākums ievērot šīs Politikas prasības, kuras attieksies uz Darbinieka ierīcēm kā uz ierīcēm, kas pieder RISEBA, ka arī jāievēro sekojošas prasības:

7.5.1. Ja ierīce paredz tādu iespēju, visi RISEBA dati jāglabā atsevišķi no citiem datiem, mapē ar individuālu šifrēšanas iespēju un/vai individuālu paroles aizsardzību.

7.5.2. RISEBA dati ir jādzēš no ierīces, kad to glabāšana vairs nav nepieciešama konkrētā darba uzdevuma izpildei.

7.6. Ja Darbinieks saņem paziņojumu par to, ka viņa izmantotajā ierīcē ir atrasts vīruss, ir stingri aizliegts piekļūt jebkuram ierīces failam, kā arī aizvērt jebkuru atvērtu logu vai paziņojuma logu un nekavējoties jāsazinās ar Resursa turētāju un jāinformē par notikušo.

7.7. Par RISEBA ierīces vai personīgās ierīces nozaudēšanu, kura tika izmantota darba pienākumu pildīšanai, nekavējoties jāinformē Resursa turētājs. Ja ierīce saturēja personas datus, par to nekavējoties jāziņo arī DAS.

8. DATU NESĒJU GLABĀŠANAS UN IZNĪCINĀŠANAS KĀRTĪBA

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

8.2. RISEBA konfidenciālos datus 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. Kad RISEBA elektroniski datu nesēji ir salauzti vai nepilda savu funkciju pilnvērtīgi, datu nesēji ir jāiznīcina.

8.5. Ja RISEBA elektroniskiem datu nesējiem ir piekļuve vairākiem Darbiniekiem, vai datu nesēji tiek nodoti lietošanai citām personām, Darbinieks, kas nodod datu nesēju, pārliecinās, ka tas nesatur RISEBA informāciju un nodod to citas personas lietošanā tikai pēc tajā esošo datu dzēšanas.

9. RESURSU DROŠĪBA

9.1. Serveru drošība (attiecas uz Resursa turētāju)

9.1.1. RISEBA datu glabāšanai un apstrādei izmantotas serveru ierīces jāizvieto izdalītas RISEBA telpās vai sadarbības partnera drošās datu centra telpās. Fiziska piekļuve serveru ierīcēm un telpām, kur tie ir izvietoti, ir atļauta Resursu turētājam un/vai sadarbības partnera tehniskā atbalsta personālam ar Resursu turētāja uzraudzību un/vai saskaņā ar sadarbības līguma nosacījumiem;

9.1.2. Piekļuvei serveru pārvaldības saskarnei ir atļauts izmantot tikai speciāli tām paredzētie administrēšanas konti;

9.1.3. Visi piekļuves gadījumi serveru resursiem un/vai pārvaldības saskarnei ir jāsaglabā auditācijas žurnālā, piefiksējot piekļuves datumu un laiku, personu vai lietotāja kontu kas veica piekļuvi, un piekļuves veidu (skatīšana, izmaiņas u.c.). Veicot konfigurācijas izmaiņas, žurnālā jāieraksta izmaiņu pamatojumu;

9.1.4. Serveru datiem un konfigurācijai regulāri jāveic rezerves kopēšanu. Katrai datu vienībai jāveido vismaz 2 kopijas, kurus jāglabā fiziski attālināti vienu no otras.

9.2. Tīkla drošība

9.2.1. RISEBA iekšējam slēgtam WiFi interneta tīklam drīkst pieslēgties tikai RISEBA darbinieki. RISEBA apmeklētājiem, sadarbības partneriem, ārštata pasniedzējiem, studentiem interneta izmantošanai ir nepieciešams pieslēgties atvērtajam WiFi viesu tīklam.

9.2.2. Strādājot attālināti, RISEBA nodrošina Darbinieku pieslēgšanas iespēju RISEBA sistēmām, izmantojot SSL VPN sistēmu.

9.2.3. Darbiniekiem Ir stingri aizliegts lietot interneta publiskos pieslēgumus (piemēram, interneta kafejnīcā, bibliotēkās utt.) piekļuvei RISEBA datiem, izņemot gadījumus, kad darba pienākumu izpilde notiek komandējumā vai tā ir kritiska un neatliekama ar darbu saistīta nepieciešamība un Darbinieka Tiešais vadītājs ir sniedzis skaidru rakstisku piekrišanu šādai darbībai. Visos citos gadījumos ir jāizmanto mobilo sakaru tīkls.

9.2.4. Izmantojot RISEBA ierīces, pārlūkošana Darbinieka 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.

9.3. Ugunsdrošība

9.3.1. RISEBA nodrošina un uztur uguns novēršanas un detektēšanas iekārtas/sistēmas, kuras strādā no neatkarīgiem enerģijas avotiem.

9.3.2. Datu centros, serveru telpās un telpās, kurās atrodas skaitļošanas iekārtas, izmanto tikai gāzveida vai pulverveida ugunsdzēšanas aparātus.

9.4. Temperatūras un mitruma kontrole

RISEBA nodrošina atbilstošu temperatūras un mitruma līmeni telpās, kurās atrodas informācijas sistēmas infrastruktūra un uzrauga temperatūras un mitruma līmeni.

10. AIZLIEGTĀS DARBĪBAS

10.1. 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 Darbinieka darba pienākumiem vai nav saistīti ar RISEBA darbību.

10.2. Ir stingri aizliegts veikt šādas darbības:

(a) Pārkāpt jebkuras personas vai uzņēmuma tiesības, kas aizsargāti 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 aprīkojumā;
(b) Neatļauti kopēt autortiesību aizsardzības objektus;
(c) Pārkāpt jebkura datu subjekta tiesības, pārmērīgi un nevajadzīgi vācot un apstrādājot šāda datu subjekta personas datus;
(d) Piekļūt datiem, serverim vai kontam ar nolūku, kas nav saistīts ar RISEBA darbības veikšanu vai Darbinieka amata pienākumu veikšanu;
(e) Eksportēt programmatūru, tehnisko informāciju, šifrēšanas programmatūru vai tehnoloģiju, pārkāpjot piemērojamos starptautiskos vai nacionālos likumus un noteikumus un / vai RISEBA norādījumus;

(f) Atklāt Darbinieka piekļuves datus RISEBA sistēmām un nodrošināt iespēju citām personām lietot personīgo kontu (ieskaitot, bet neierobežojoties ar darbinieku 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 Darbiniekam, vai Darbinieka ielogošanās vai piekļuve serverim vai kontam bez speciālās atļaujas, ja vien šādi pienākumi nav Darbinieka amata pienākumi vai piekļuves tiesības Darbiniekam tiek piešķirtas sakarā ar atsevišķu RISEBA projektu;
(i) Izmantot jebkuru programmu / skriptu / komandu vai sūtīt jebkura veida ziņojumus ar mērķi traucēt vai atspējot lietotāja sesiju.

11. DROŠĪBAS PĀRKĀPUMU INCIDENTU PAZIŅOŠANA UN APSTRĀDE

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

11.2. 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.

11.3. Resursa turētājam un DAS ir pienākums nodrošināt laicīgu ziņošanu par informācijas drošības pārkāpumiem saskaņā ar Latvijas un ES normatīvajos aktos noteikto.

11.4. RISEBA izmeklē un dokumentē katru informācija sistēmu drošības incidentu. Informācijas sistēmu drošības incidentu dokumentācijā uztur uzskaiti par katru incidentu, statusu, un citu noderīgu informāciju, kas nepieciešama, lai varētu izmeklēt incidentu iemeslus.

11.5. Drošības pārkāpumu incidentus apstrādā, ietverot Incidentu identifikāciju un analīzi, novēršanu un atjaunošanu. Iegūto pieredzi dokumentē un to izmanto treniņa un testēšanas uzdevumos.

12. INCIDENTU NOVĒRŠANAS PLĀNS

Lai adekvāti reaģētu uz incidentiem, Resursa turētājs nodrošina incidentu novēršanas plāna izstrādi, ieviešanu, uzturēšanu un regulāru pārskatīšanu. Nepieciešamības gadījumā incidentu novēršanas plāns ir jāatjauno.

13. PĀRVALDĪBA UN ATSKAITES

13.1. Resursa turētājs atbild par:
1. informācijas sistēmu drošības pārvaldīšanu un Politikas uzturēšanas uzraudzību, nodrošinot pasākumus, kas veicina RISEBA informācija sistēmu drošības integritāti un neievainojamību, regulāri pārskatot un izmantojot jaunākos tehnoloģijas sasniegumus, kā arī pilnvērtīgi izmantojot pieejamos resursus;
2. Politikas uzturēšanu un atjaunošanu, pieaicinot DAS. Politiku pārskata regulāri un vismaz reizi gadā, kā arī katru reizi, kad RISEBA maina, papildina, groza vai citādi izmaina esošos IT resursus un sistēmas;
3. risku izvērtēšanu un iekšējo auditu. Minētās darbības jāveic kopā ar DAS pēc nepieciešamības;
4. drošības pārkāpumu novēršanu un incidentu pārvaldību;
5. drošības pārkāpumu protokolēšanu un atspoguļošanu informācijas sistēmu drošības incidentu reģistrā.

13.2. Pirms informācijas sistēmu vai tās komponentu nodošanas tehniskai apkopei vai remontam, Resursa turētājs pārbauda vai tās nesatur konfidenciālu informāciju vai personas datus. Ja satur, tad ir jānodrošina visu iespējamo, lai nodrošinātu informācijas konfidencialitāti (piem., šifrēšana, anonimizācija).

13.3. Pēc tehniskās apkopes vai remonta pasākumiem Resursa turētājs pārbauda visas potenciāli ietekmējamās drošības kontroles, lai pārliecinātos par to darbību. Datu nesēju bojājuma gadījumā jāpārliecinās, ka dati no datu nesējiem nav atjaunojami un tā remonta gadījumā dati nenokļūs trešo personu rīcībā.

13.4. Resursa turētājs uztur saziņu ar personām, kas nodrošina Informācijas sistēmu drošības uzturēšanas pakalpojumus, kā arī pārliecinās, ka šādām personām ir saistoši informācijas neizpaušanas nosacījumi, ja šādām personālam ir nepieciešamība piekļūt konfidenciālai informācijai.

13.5. Veicot kārtējo datu aizsardzības atbilstības pārbaudi, DAS pieprasa un Resursa turētājam ir pienākums sniegt visu informāciju, kura ir nepieciešama DAS, lai izvērtētu vai tiek sasniegti Politikas mērķi un vai notiek nepārtraukta Politikas noteikumu ievērošana. Iegūto informāciju kopā ar citu datu aizsardzības procesa atbilstības informāciju DAS apkopo un iesniedz RISEBA Rektoram/-ei vismaz reizi gadā.

14. DARBINIEKU APMĀCĪBAS

14.1. Administratīvais direktors organizē regulārās - ne retāk kā reizi gadā - Darbinieku apmācības par kiberdrošību, kas iekļauj, bet neierobežojas ar:

- informāciju par interneta krāpniecības riskiem un veidiem, aizliegtām darbībām un citu aktuālo informāciju informācijas drošības jomā, kura veicina Darbinieku izpratni un drošu darbu ar RISEBA ierīcēm un sistēmām;
- bāzes zināšanas, kas nepieciešamas, lai nodrošinātu informācijas sistēmas drošību un Darbinieku uzvedību atbilstoši pieņemtajām RISEBA drošības prasībām, kas citu starpā palīdz atpazīt un reaģēt uz aizdomīgiem drošības incidentiem;
- informāciju, kas nepieciešama drošības procesu realizācijai un kas atbilst Politikas noteikumiem.

14.2. Informāciju par apmācībām dokumentē un glabā 7 gadus.

15. NOSLĒGUMA NOTEIKUMI

15.1. Politika stājas spēkā tās apstiprināšanas dienā. Vadības un Tiešā vadītāja pienākums ir pārliecināties par to, ka Darbinieks ir iepazinies ar Politikas noteikumiem. Ja normatīvie akti nenosaka citādi, Darbinieki tiek iepazīstināti ar šo Politiku elektroniski vai papīra formā, un tiks uzskatīts, ka Politika kļuva pieejama Darbiniekam, Darbinieks ir iepazinies ar tās noteikumiem un Politika ir saistoša tās 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 politika				
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