LATVIJAS UNIVERSITĀTES AĢENTŪRA
LATVIJAS UNIVERSITĀTES P. STRADIŅA MEDICĪNAS KOLEDŽA
Reģistrācijas Nr. 90000031813, Vidus prospekts 38, Jūrmala, LV-2010
Tālrunis 67752507, fakss 67752214, e-pasts: st-skola@apollo.lv

APSTIPRINĀTS
Latvijas Universitātes
P.Stradiņa medicīnas koledžas padomes
2020. gada 21. janvārī sēdē, prot. Nr. 1

INFORMĀCIJAS DROŠĪBAS POLITIKA

Jūrmalā

Izdota saskaņā ar Vispārīgo datu aizsardzības regulu un Fizisko personu datu apstrādes likumu

1. Lietoto terminu definīcijas

Koledža	Latvijas Universitātes P. Stradiņa medicīnas koledža, Reģ.Nr.90000031813, Vidus prospekts 38, Jūrmala, LV-2010.
Darbinieks	Koledžā nodarbināta fiziska persona.
Tiešais vadītājs	Koledžas pārstāvis, kurš ir norādīts attiecīgā Darbinieka Darba vai citā līgumā vai iecelts ar Koledžaas rīkojumu kā Darbinieka tiešais vadītājs.
Vadība	Administrācija un/vai jebkura cita persona Koledžā, kurai piešķirtas vadības funkcijas un pilnvaras.
Politika	Šī Informācijas drošības politika.
Trešā persona	Fiziska vai juridiska persona, kas nav Koledžas darbinieks.
Tīkla drošības pārkāpums	Šādi drošības pārkāpumi iekļauj, bet 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 Koledžas projektā;
Autortiesības	Autora personisko nemantisko un mantisko tiesību kopums uz paša radītu intelektuālo darbu tā materiālajā formā.
Informācija	Ziņa vai ziņu kopums jebkurā tehniski iespējamā fiksēšanas, uzglabāšanas vai nodošanas veidā.
Personas dati	Jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjekts"); 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.
Personas identifikācijas dati	Vārds, uzvārds, personas kods, dzimšanas dati.
Datu subjekts	Identificēta vai identificējama fiziskā persona.
Serveris	Dators jeb sistēma, kas nodod informāciju citiem datoriem sauktiem par klientiem. Šie klienti var piekļūt servera datoram vainu caur lokālo tīklu) vai internetu.

Konts	Drošības mehānisms, ko izmanto, lai kontrolētu piekļuvi datoru sistēmai vai tīklam. Lietotāja kontā ietilpst informācija par lietotāja vārdu, paroli, tā tiesībām un, iespējams, cita informācija, kas ļauj identificēt lietotāju.
IT	Informācijas tehnoloģijas
Lietotāja ID	Unikāls klienta identifikators, pēc kura Koledža identificē lietotājus, kas piekļūst Informācijas sistēmām.
Informācijas sistēma	Strukturizēts informācijas tehnoloģiju un datu bāzu kopums (piemēram, bet ne tikai, datortehnika, programmatūra, operētājsistēmas, jebkura uzglabāšanas vide, tīkla konti, elektroniskā pasta konti, pārlūku sistēmas), kuru lietojot tiek nodrošināta Koledžas funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

2. Mērķis un apjoms

2.1. Koledžas informācijas drošības sistēmas mērķis ir pasargāt Koledžas darbiniekus, partnerus un studentus 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. Politika regulē informācijas apstrādi jebkurā informācijas sistēmā, kas Iestādē iesaistīti datu/informācijas apstrādē neatkarīgi no tā, vai datu/informācijas apstrāde ir saistīta ar Koledžas iekšējo darbību vai Koledžas ārējām attiecībām ar jebkuru Trešo personu.

2.3. Šī Politika regulē arī to, kā Koledžas Darbinieki lieto viņiem pieejamo aprīkojumu un rīkus savu darba pienākumu veikšanai.

2.4. Politika var būt piemērojama kopā ar jebkurām citām politikām, noteikumiem, procedūrām un/vai vadlīnijām, ko periodiski pieņem un ievieš Koledža.

2.5. Par visiem informācijas drošības sistēmas jautājumiem un informācijas/datu drošības jautājumiem, kas nav minēti šajā Politikā, Darbiniekiem ir jāvēršas pie datortīkla uzturēšanas administratora.

2.6. Ar šo Politiku rakstveidā jāiepazīstina visi Darbinieki un jāpārliecinās, ka viņi tos ir izpratuši. Nepieciešamības gadījumā ir jāorganizē darbinieku mācības vienotas un pareizas izpratnes radīšanai par IT un personas datu aizsardzības jautājumiem.

3. Informācijas klasifikācija

3.1. Jebkuru informāciju/datus, kas kļūst pieejami Darbiniekiem, veicot savus darba pienākumus, ja šāda informācija/dati ir saistīti ar Koledžu un tās darbību, darbiniekiem, studentiem vai sadarbības partneriem, uzskata par Koledžai piederošu un konfidenciālu informāciju, ko aizsargā atbilstoši piemērojami normatīvie akti par konfidenciālas informācijas un personas datu aizsardzību.

3.2. Lai nodrošinātu informācijas un datu aizsardzību, Koledža veic iekšējo informācijas klasifikāciju. Informāciju/datus aizsargā neatkarīgi no tā vai šāda informācija ir nonākusi Darbinieka rīcībā drukātā, elektroniskā, vai jebkurā citā veidā.

3.3. Koledža lieto šādu vispārīgu informācijas klasifikāciju:

Kategorija	Apraksts	Saturs
Publiska informācija	Informācija, kuru var izstrādāt, apstrādāt un izplatīt Koledžas iekšienē vai ārpus tās bez jebkādas negatīvas ietekmes uz Koledžu, jebkuru no tās Darbiniekiem, studējošiem un /vai sadarbības partneriem.	a) Publiski finanšu pārskati, ko sniedz valsts iestādēm. b) Informācija, kas pieejama publiskos resursos vai ir kā citādi publiski zināma, ja vien tā nav kļuvusi publiski zināma tādēļ, ka Darbinieks rīkojies, pārkāpjot informācijas/datu drošības prasības.
Iekšējā informācija	Jebkura informācija, kuras jebkāda veida lietošana, ja tas notiek, pārkāpjot piemērojamos normatīvos aktus, šīs Politikas vai jebkura cita Koledžas pieņemta regulējuma prasības, var kaitēt Koledžas jebkura tās Darbinieka, studējošā un/vai sadarbības partnera interesēm.	a) Jebkura Koledžas Darbinieka, struktūrvienības izstrādāti un/vai sagatavoti dokumenti. b) Jebkādi Koledžas darbības mērķiem izveidoti un/vai lietoti katalogi (kontaktu, informācijas u. tml.). c) Jebkurš iekšējs dokuments, kas izstrādāts Koledžas darbības vajadzībām.
Konfidenciāla informācija	Jebkura informācija, kas ir tik būtiska Koledžai, ikvienam tās Darbiniekam, studējošam un /vai sadarbības partneriem, kuras neautorizēta izpaušana var negatīvi ietekmēt Koledžas, tās Darbinieku, studējošo un/vai sadarbības partneru komercdarbību, reputāciju, statusu kopumā, un šādas izpaušanas rezultātā jebkurai no šīm personām var tikt nodarīts nopietns kaitējums.	a) Politikas, procedūras, iekšējie noteikumi, vadības lēmumi (izņemot tos dokumentus, kuru publicēšanas nepieciešamību nosaka normatīvie akti). b) Informācija, kas Darbiniekam norādīta kā ierobežotas pieejamības informācija. c) Personas identifikācijas dati. d) Informācija, ko aizsargā katra Darbinieka parakstīta konfidencialitātes vienošanās (ja tāda ir parakstīta). e) Informācija, ko aizsargā konfidencialitātes vienošanās vai sadarbības līgumi, ko Koledža ir noslēgusi savas darbības gaitā.

4. Datu/informācijas apstrādē iesaistītās sistēmas

4.1. Jebkura informācija/dati, ko izmanto Koledžas darbībā, uzskatāmi par Koledžas īpašumu. Jebkādas informācijas sistēmas, tostarp, bet ne tikai datortehnika, jebkādas uzglabāšanas vides, tīkla konti, jebkāda cita tehniskā bāze un rīki, ko izmanto Koledžas darbībā, uzskatāmi par Koledžas īpašumu.

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

4.3. Koledžas lietotajā aprīkojumā var instalēt un lietot tikai Koledžas 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.

4.4. Koledža auditē informācijas/datu apstrādē izmantotās sistēmas, lai kontrolētu nepārtrauktu atbilstību šai Politikai un piemērojamajām normatīvo aktu prasībām.

5. Darbinieku pienākumi

5.1. Jebkura 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 nevienai Trešajai personai, 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 veikšanai ar nosacījumu, ka šādas darbības tiek veiktas Darbiniekam piešķirto pilnvaru robežās un saskaņā ar normatīvajos aktos 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. Jebkuru informācijas/datu pieprasījumu un/vai pieprasījumu par informācijas/datu apstrādi, ko Darbinieks, veicot savus darba pienākumus, ir saņēmis no datu subjektiem, nekavējoties pārsūta turpmākai izskatīšanai Vadībai.

5.4. Ikvienam Darbiniekam ir pienākums ievērot šo Politiku, kā arī pildīt spēkā esošo Latvijas Republikas vai starptautisko normatīvo aktu (piemēram, Darba likums, Fizisko personu datu apstrādes likums, Vispārējā datu aizsardzības regula u.c.) prasības, kas paredz informācijas/datu apstrādes un to aizsardzības nosacījumus.

5.5. Politikas neievērošana tiek uzskatīta par būtisku noteiktās darba kārtības pārkāpumu un tā rezultātā, pēc Koledžas ieskatiem, Darbiniekam var piemērot disciplinārsodu vai uzteikt Darbiniekam darbu. Tas var izraisīt pārkāpumu pieļāvušā Darbinieka saukšanu pie administratīvās vai krimināls atbildības.

6. Piekļuves un aizsardzības pārvaldība

6.1. Darbinieki var piekļūt jebkurai Koledžas ierīcei, ja tas nepieciešams attiecīgo Darbinieku darba pienākumu veikšanai, atbildības ietvaros. Piekļuves tiesības jebkurai informācijas sistēmai nenozīmē, ka Darbinieks ir pilnvarots apskatīt vai lietot visu attiecīgajā sistēmā esošo informāciju – Darbiniekiem ir tiesības lietot tikai tiešo darba pienākumu izpildei nepieciešamos datus.

6.2. Darbiniekus identificē lietotāja ID. Ikviens Darbinieks atbild par visām darbībām, kas saistītas ar lietotāja ID, tādēļ primārais pienākums ir nodrošināt, lai Lietotāja ID nebūtu pieejams nevienai Trešajai personai un citiem Darbiniekiem, ja vien Koledža nav noteikusi citu kārtību.

6.3. Sistēmas drošības paroles tiek izveidotas ar nosacījumu, ka tās nevar viegli atminēt, tās sastāv vismaz no 9 simboliem (tostarp, lielajiem un mazajiem burtiem, cipariem, kā arī speciālajiem simboliem), tās neietver personas datus. Drošības paroles tiek regulāri mainītas (vismaz reizi 3 (trīs) mēnešos). Ikviens Darbinieks personīgi atbild par savas drošības paroles atbilstību šai Politikai un pārējiem Koledžas noteikumiem.

6.4. Darbinieks piekļūst konfidenciālai informācijai/datiem tikai tad, ja šādas pilnvaras ir paredzētas attiecīgā Darbinieka Darba vai citā līgumā un/vai ja Koledža ir piešķīrusi Darbiniekam šādas pilnvaras.

7. Drošības pasākumi

7.1. Visiem jebkurā formā (drukātā, elektroniskā u. tml.) ievāktiem un apstrādātiem datiem un informācijai piemērojamas šīs Politikas un jebkura normatīvā regulējuma prasības attiecībā uz datu/informācijas ievākšanu, apstrādi, aizsardzību un uzglabāšanu, un šādus dokumentus uzglabā Koledžas norādītā drošā vietā ar tādu uzglabāšanas termiņu, kādu paredz piemērojamie likumi (piemēram, Darba likums, Augstskolu likums, Fizisko personu datu apstrādes likums u.c.) un/vai norāda Koledža.

7.2. Darbiniekiem aizliegts glabāt konfidenciālu informāciju savās personiskajās ierīcēs, izņemot informāciju, kas ir īslaicīgi nepieciešama konkrētai, ar darbu saistītai darbībai. Visa nepieciešamā konfidenciālā informācija jāuzglabā tikai Koledžas IT personāla apstiprinātā vietā uz servera. Ir jāizvairās no jebkādas šādu datu lejupielādēšanas datoros, un tas jādara tikai tad, ja ir pamatota nepieciešamība saistībā ar informācijas apstrādi darba vajadzībām.

7.3. Ja Koledžai rodas pamatotas aizdomas, ka kāds darbinieks ir veicis nepamatotu datu apstrādi, Koledžas 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 jebkurai informācijas uzglabāšanas vietai uz servera jābūt Koledžas IT personāla apstiprinātai, lai novērstu neautorizētu piekļuvi.

7.5. Gadījumos, kad Darbinieki lieto personīgās (mājas) ierīces, lai piekļūtu Koledžas korporatīvajiem resursiem (piemēram, elektroniskais pasts, tiešsaistes /datubāzes), Darbiniekiem ir pienākums ievērot šīs Politikas prasības tieši tāpat kā lietojot Koledžas nodrošināto aprīkojumu. Personīgā (mājas) ierīcē ir aizliegts glabāt jebkādus ar Koledžu saistītus personas datus. Jebkura datu apstrāde ir pieļaujama tikai ar Koledžas lietoto tiešsaistes glabāšanas vietu starpniecību.

7.6. Darba vajadzībām 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.

7.7. Gadījumā, ja Darbiniekam tiek piešķirtas tiesības piekļūt Koledžas sadarbības partnera datņu glabāšanas sistēmai, Darbiniekam ir pienākums lietot piešķirto ID 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.).

7.8. Tiklīdz, pēc Koledžas ieskatiem, aizsargātie dati/informācija vairs nav nepieciešama Koledžas darbībai, šādi dati/informācija tiek dzēsta, iznīcinātas visas to kopijas un attiecīgās informācijas/datu apstrādē iesaistītajiem Darbiniekiem ir pienākums dzēst/iznīcināt un nodot tiešajam vadītājam Koledžas informāciju/datus, kas viņiem vairs nav nepieciešami savu darba pienākumu veikšanai, jo īpaši, ja ar attiecīgo Darbinieku tiek izbeigtas darba tiesiskās attiecības.

7.9. Nekādu šajā Politikā minēto informāciju/datus nenosūta, nepārsūta un nekādā citā veidā neiesniedz Trešajai personai ja vien tas nav nepieciešams Darbinieka darba pienākumu izpildei. Gadījumā, ja datus pārsūta vai iesniedz Trešajai personai ir jānodrošina datu aizsardzība un jāveic visi atbilstošie drošības pasākumi.

7.10. IT speciālistam ir jāveic informācijas sistēmu risku analīze (gan pirms šo sistēmu ekspluatācijas sākšanas, gan regulāri – vismaz reizi gadā). Riska analīze ir jādokumentē.

7.11. IT speciālistam ir jānodrošina regulāra informācijas sistēmas notikumu reģistrēšana un monitorēšana.

8. Aizliegtās darbības

8.1. Nekādu Koledžai piederošu aprīkojumu vai sistēmas nekādā gadījumā un nekādos apstākļos nedrīkst izmantot ar Darbinieka darba pienākumiem vai ar Koledžas darbību nesaistītiem mērķiem.

8.2. Turpmāk minētās darbības ir stingri aizliegtas:

8.2.1. jebkuras personas vai Koledžas ar autortiesībām aizsargātu tiesību pārkāpšana, tostarp (bet ne tikai), jebkuras nelegālas programmatūras, tiešsaistes platformu, jebkura cita elektroniskā satura, kuru Koledža nav licencēta lietot, uzstādīšana, kopēšana, izplatīšana vai uzglabāšana jebkurā Koledžas sistēmā vai aprīkojumā;

8.2.2. jebkuras personas tiesību aizskaršana, pārmērīgi un bez vajadzības ievācot un apstrādājot attiecīgā datu subjekta personas datus;

8.2.3. piekļuve Personas datiem tādiem mērķiem, kas nav saistīti ar Koledžas darbību vai attiecīgā Darbinieka darba pienākumu veikšanu;

8.2.4. programmatūras, tehniskās informācijas, šifrēšanas programmatūras vai tehnoloģijas eksportēšana, pārkāpjot šo Politiku;

8.2.5. jebkādu datu vai informācijas, kurai Koledžas ir īpašuma tiesības un/vai konfidenciāla vērtība, eksportēšana, ja tā nav nepieciešama Koledžas darbības vai Darbinieka darba pienākumu veikšanas gaitā un/vai tā pārkāpj Koledžas iekšējos noteikumus un piemērojamos normatīvos aktus;

8.2.6. Darbinieka paroles atklāšana citām personām un atļauja citām personām lietot darbinieka kontu (tostarp, bet neaprobežojoties ar Darbinieka ģimenes locekļiem);

8.2.7. tīkla sakaru drošības pārkāpumu vai pārtraukumu īstenošana;

8.2.8. jebkuras programmas lietošana vai jebkāda veida ziņojuma nosūtīšana ar nolūku traucēt lietotāja darba sesiju.

9. Ziņošana par drošības incidentiem

9.1. Par visiem informācijas/datu apstrādes drošības incidentiem vai iespējamiem incidentiem nekavējoties ir jāziņo Vadībai, kas veic pasākumus iespējamā kaitējuma novēršanai, radītā kaitējuma seku likvidēšanai un iepriekšējā drošības stāvokļa atjaunošanai.

9.2. Personas datu aizsardzības pārkāpuma gadījumā Koledžas Vadība ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tai kļuvis zināms, paziņo par personas datu aizsardzības pārkāpumu Datu valsts inspekcijai, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums var radīt risku fizisku personu tiesībām.

9.3. Koledža dokumentē visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar personas datu pārkāpumu, tā sekas un veiktās koriģējošās darbības.

9.4. Koledža veic nepieciešamās darbības, lai novērstu identiska vai līdzīga drošības incidenta atkārtošanos.

10. Noslēguma jautājumi

10.1. Koledža nodrošina Koledžas darbiniekiem pieeju Politikai Koledžas serverī "Iekšējā kvalitātes nodrošināšanas sistēma".

10.2. Šī Politika "Informācijas drošības politika" stājas spēkā 2020. gada 21. janvārī.