Apstiprināts ar Alberta koledžas direktora
2025.gada 02. maija rīkojumu Nr. Nr. 2-09/25-15

# INFORMĀCIJAS DROŠĪBAS POLITIKA

## 1. Vispārīgie jautājumi

1.1. Informācijas drošības politikas (turpmāk tekstā – Politikas) mērķis ir noteikt principus visas Alberta koledžas (turpmāk tekstā – Koledžas) informācijas un saistīto tehnoloģisko resursu drošības sasniegšanai, ar mērķi:
- 1.1.1. Aizsargāt vērtīgus Koledžas informācijas resursus;
- 1.1.2. Aizsargāt Koledžas darbinieku, studentu, partneru un piegādātāju informāciju;
- 1.1.3. Nodrošināt informācijas pieejamību, integritāti, konfidencialitāti;
- 1.1.4. Pārvaldīt drošības apdraudējumus;
- 1.1.5. Identificēt un minimizēt drošības incidentus;
- 1.1.6. Atjaunot sistēmu darbību pēc drošības incidentiem.

1.2. Politika ir izstrādāta kā pamata dokuments, kas nosaka galvenos drošības pamatnosacījumus informācijas tehnoloģijas videi un definē kārtību informācijas un tehnoloģisko resursu konfidencialitātes, integritātes un pieejamības nodrošināšanai.

1.3. Izstrādājot vai koriģējot Koledžas iekšējos reglamentējošos dokumentus, ir jāievēro Politikas noteiktās normas un principi.

1.4. Politika ir saistoša visiem Koledžas darbiniekiem un tās studentiem.

## 2. Informācijas drošības politikas mērķi un pamatnostādnes

2.1. Nodrošināt tādu informācijas tehnoloģiju vidi, lai Sistēma (termins "Sistēma" iekļauj visas Koledžas informācijas sistēmas, programmatūru un to saistīto infrastruktūru, piemēram, e-pasts, e-studiju vide, Moodle, Office365, operētājsistēma Windows u.c.) būtu aizsargāta pret ārējiem un iekšējiem drošības apdraudējumiem.

2.2. Apliecināt Koledžas vadības atbalstu informācijas drošības nodrošināšanai, atbilstoši Koledžas vajadzībām, saistošajiem normatīvajiem aktiem un drošības normām.

2.3. Informācijas drošības politika ir saistoša visiem Sistēmas lietotājiem.

## 3. Informācijas drošības politikas uzdevumi

3.1. Nodrošināt informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas).

3.2. Nodrošināt informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu).

3.3. Nodrošināt informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot).

3.4. Aizsargāt Sistēmas informācijas resursus.

3.5. Aizsargāt Sistēmas tehniskos resursus.

3.6. Noteikt Sistēmas drošības apdraudējumus.

3.7. Novērtēt Sistēmas drošības riskus.

3.8. Atklāt Sistēmas drošības incidentus.

3.9. Atjaunot Sistēmas darbību pēc sistēmas drošības incidentiem.

## 4. Informācijas drošības pārvaldības organizācijas principi

4.1. Augstskolā ir noteikts un patstāvīgi tiek pilnveidots dokumentu un pasākumu kopums, kuru īstenošana nodrošina informācijas drošības politikas mērķa sasniegšanu.

4.2. Koledža veicina katra darbinieka un studenta izpratni par pienākumiem risku un darbības nepārtrauktības pārvaldīšanā un informācijas un tehnisko resursu aizsardzības nodrošināšanā, veicot Koledžas darbinieku un studentu regulāru izglītošanu.

4.3. Koledža nodrošina pastāvīgu informācijas drošības politikas īstenošanas koordinēšanu un pārraudzīšanu.

4.4. Gadījumos, kad Koledžas darbinieki vai studenti neievēro Politikas izvirzītās prasības, Koledžas vadība var ierosināt disciplinārās atbildības procesu saskaņā ar normatīvajiem aktiem. Papildus tam atsevišķos gadījumos patvaļīgi piekļūstot Informācijas sistēmām, veicot darbības traucējumus un citas nesankcionētas darbības var tikt piemērota krimināltatbildība ņemot vērā, piemēram, Krimināllikuma 241, 243, 245 pantu.

4.5. Augstskolā ir skaidri definēts un izprasts atbildības sadalījums par informācijas drošību:

4.6. Koledžas vadība:

- 4.6.1. Atbild par informācijas drošību;
- 4.6.2. Nosaka un apstiprina informācijas drošības politiku;
- 4.6.3. Nodrošina nepieciešamos līdzekļus un atbalstu informācijas drošības politikas ieviešanai, uzturēšanai un pilnveidošanai;
- 4.6.4. Nosaka pienākumu un atbildības sadalījumu attiecībā uz informācijas drošību:
  - 4.6.4.1. Atbildīgā persona par informācijas drošības pārvaldību ir Koledžas IT nodaļas vadītājs;
  - 4.6.4.2. Sistēmas tehnisko resursu valdītājs ir IT nodaļas vadītājs;
  - 4.6.4.3. Sistēmas informācijas resursu valdītājs ir IT nodaļas vadītājs.

4.7. Atbildīgā persona par informācijas drošības pārvaldību:

- 4.7.1. Organizē informācijas risku analīzes veikšanu;
- 4.7.2. Nodrošina nepieciešamo informācijas drošības dokumentu uzturēšanu un īstenošanu;
- 4.7.3. Veic noteikto drošības prasību ievērošanas uzraudzību un drošības incidentu izmeklēšanu;
- 4.7.4. Nodrošina darbinieku apmācību informācijas drošības jomā.

4.8. Sistēmas tehnisko resursu valdītājs:

- 4.8.1. Atbild par Sistēmas tehnisko resursu iegādi, izstrādi, darbību un uzturēšanu;
- 4.8.2. Nodrošina Sistēmas tehniskos un loģiskos aizsardzības pasākumus;
- 4.8.3. Atbild par Sistēmas pieejas tiesību pārvaldību;
- 4.8.4. Veic Sistēmas darbības atjaunošanas pasākumus, ja Sistēmas darbība ir traucēta.

4.9. Sistēmas informācijas resursu valdītājs:

- 4.9.1. Atbild par pieejas kontroles politikas noteikšanu informācijas resursam;
- 4.9.2. Klasificē viņa pārziņā esošos informācijas resursus;
- 4.9.3. Nosaka drošības prasības informācijas resursam.

4.10. Lietotāji:

- 4.10.1. Iepazīstas un apņemas ievērot iekšējo normatīvo aktu prasības informācijas drošības jomā;

4.10.2. Ziņo par Sistēmā identificētajiem riskiem, informācijas drošības notikumiem un incidentiem.

## 5. Informācijas drošības atbilstība normatīvajiem aktiem un standartiem

5.1. Sistēma atbilst Latvijas Republikas tiesību aktiem informācijas drošības jomā:

5.1.1. Sistēmā ir ievērotas Latvijas Republikas normatīvo aktu prasības informācijas tehnoloģiju un informācijas drošības jomā (tostarp ievērotas fizisko personas datu aizsardzības prasības).

5.2. Sistēma atbilst starptautiskajiem normatīvajiem aktiem un standartiem informācijas drošības jomā.

## 6. Informācijas drošības principi

6.1. Sistēmas lietotāju konti:

6.1.1. Sistēmas lietotāji, kas veic Sistēmas administrēšanas darbu, izmanto tam īpašus lietotāju kontus (turpmāk – Sistēmas administratora konti), kas netiek izmantoti ikdienas darbību veikšanai;

6.1.2. Katrs lietotāja konts ir saistīts ar konkrētu fizisko personu;

6.1.3. Sistēmkontus aizsargā tā, lai novērstu iespēju lietotājiem tos izmantot;

6.1.4. Ar administratora kontu piekļūt Sistēmai iespējams tikai izmantojot iekārtas, kas atrodas Koledžas kontrolētās telpās;

6.1.5. Sistēmas lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju - kļūdas apraksts un kļūdas identifikators.

6.2. Prasības parolēm:

6.2.1. Piekļuve Sistēmai ir aizsargāta ar lietotāja vārdu un paroli;

6.2.2. Sistēmas lietotāja paroļu garums nav mazāks par trīspadsmit simboliem un satur vismaz lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un citu simbolu;

6.2.3. Katram Sistēmas lietotājam parole ir obligāti jāmaina pēc ne vairāk kā 90 dienām;

6.2.4. Piecas secīgas reizes nepareizi ievadot sistēmas lietotāja konta paroli, šis konts (izņemot Sistēmas administratora kontu) nekavējoties tiek bloķēts;

6.2.5. Sistēmas lietotāja paroles aizliegts glabāt un transportēt nešifrētā veidā, t.sk. lietotāja autentifikācijas procesa ietvaros;

6.2.6. Sistēmas lietotāja parole tās ievadīšanas brīdī netiek pilnībā attēlota lietotājam;

6.2.7. Sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir vienreiz lietojama;

6.2.8. Sistēmā nav funkcionalitātes, kas atļauj Sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;

6.2.9. Tehnisko resursu valdītājs nodrošina, ka iekārtām, t.sk. infrastruktūras iekārtām, kas nodrošina Sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;

6.2.10. Publiski pieejamiem resursiem un/vai Sistēmās kurās pieejami klasificēti dati vai ir augsta drošības riska Sistēmas ir jāpiemēro divfaktoru autentifikācija (2FA).

6.3. Izsekojamība:

6.3.1. Tiek nodrošināta Sistēmas pierakstu veidošana un uzglabāšana vismaz 18 mēnešus pēc ieraksta izdarīšanas, uzglabājot pierakstu kopijas atsevišķi no Sistēmas;

6.3.2. Sistēmas pieraksti tiek veidoti, nodrošinot, ka ierakstā norādītais laiks sakrīt ar faktiskā notikuma koordinēto universālo laiku (UTC) ar vienas sekundes precizitāti izmantojot NTP serveri;

6.3.3. Atbildīgā persona par Sistēmas drošības pārvaldību nodrošina Sistēmas auditācijas pierakstu satura plānveida uzraudzību un analīzi, lai konstatētu incidentus;

6.3.4. Jebkura piekļuve Sistēmai ir izsekojama līdz konkrētam Sistēmas lietotāja kontam vai interneta protokola (IP) adresei.

6.4. Atjauninājumi:

6.4.1. Tehnisko resursu valdītājs sadarbībā ar atbildīgo par informācijas drošības pārvaldību veic pieejamo programmatūras atjauninājumu izvērtēšanu un nepieciešamības gadījumā - testēšanu;

6.4.2. Sistēmai jābūt uzliktiem visiem pieejamajiem nepieciešamajiem programmatūras atjauninājumiem.

## 7. Informācijas resursi

7.1. No Sistēmas atļauts pieprasīt tikai darba funkcijām nepieciešamo informāciju un datus.

7.2. Informācijas resursos pieejamās informācijas skatīšanās, drukāšana, glabāšana savā personīgajā datorā, uz serveriem vai citiem resursiem ārpus Koledžas datu glabāšanas vietas un citās elektroniskajās ierīcēs vai datu nesējos ir aizliegta, ja vien to neparedz tiešie amata pienākumi vai darba specifika.

7.3. Pieslēgt ārējos datu nesējus pie darba datora ir aizliegts. Izņēmumu gadījumi tiek izskatīti individuāli, tos piesaka caur IT atbalsta dienestu un saņemot drošības pārvaldnieka apstiprinājumu.

7.4. Privātos datu nesējus (piemēra, USB zibatmiņa, ārējie cietie diski u.c.) ir aizliegts izmantot. Datu nesēji var tikt izmantoti tikai tad, ja ir saņemta atļauja no IT nodaļas vadītāja un datu nesējs ir šifrēts un reģistrēts IT nodaļā.

7.5. Sistēmā var tikt uzkrāta informācija par jebkādām lietotāja veiktajām darbībām. Šī informācija var tikt izmantota, izmeklējot informācijas drošības pārkāpumus un citus incidentus, ievērojot normatīvajos aktos noteikto kārtību.

7.6. Informāciju nedrīkst glabāt datorā uz cietā diska. Informācija ir jāglabā uz Koledžas norādīto datņu glabāšanas vietu.

7.7. Privātos datus nedrīkst glabāt uz Koledžas piešķirtajiem datoriem.

7.8. Darbiniekiem ir jāievēro arī "tīra galda" politika, kas nozīmē, to ka konfidenciāla informācija netiek atstāta bez uzraudzības un tā vienmēr tiek droši aizsargāta, ja darba vieta tiek pamesta.

7.9. Datoriem laikā, kad tie neatrodas pie lietotāja, dators vai tā ekrāns ir jāaizslēdz (angl. - "*Lock computer*" ar tastatūras taustiņu kombināciju CTRL+ALT+DELETE vai Windows + L).

## 8. Informācijas aizsardzības pasākumi

8.1. Visās Koledžas valdījumā esošajās gala lietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos Sistēmai, ir iekļauta pretvīrusu funkcionalitāte, izmantojot antīvīrusa programatūru.

8.2. Sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamo tiesību kopu.

8.3. Fiziski piekļūt iekārtām, kas nodrošina Sistēmas darbību, atļauts vienīgi Koledžas pilnvarotām personām vai šo personu pavadībā.
8.4. Plūsma starp informācijas sistēmu un tās lietotājiem, kā arī starp informācijas sistēmu un citām informācijas sistēmām tiek kontrolēta, izmantojot ugunsmūra risinājumu un datu šifrēšanu.
8.5. Veicot Sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu Sistēmās glabāto datu integritātei, tādēļ šādiem nolūkiem ir izveidota Sistēmas testa vide.
8.6. Sistēmas izvietošana ārpakalpojumu sniedzēja nodrošinātos resursos atļauta tikai tad, ja pakalpojumu sniedzējs ir juridiska persona, kas reģistrēta Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, un Sistēmā glabātā informācija atrodas vienīgi Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā. Papildus tam Koledža nodrošina piegādes ķēdes drošību veicot nepārtrauktu piegādes ķēdes risku analīzi, uzraudzību un kontroli.
8.7. Visām Koledžas darbībām nozīmīgām Sistēmām tiek nodrošināta darbības nepārtrauktība un atjaunošanās veicot regulāras rezerves kopijas un ieviešot kontroles Koledžas darbības nepārtrauktībai.

## 9. Informācijas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamais līmenis

9.1. Atbildīgais par informācijas drošības pārvaldību ne retāk kā reizi gadā veic informācijas drošības risku analīzi.
9.2. Risku analīzes ietvaros sadarbībā ar Koledžas vadītāju tiek veikts izvērtējums, vai risku ierobežošanas un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties šo risku īstenošanās vai Koledžas darbības pārtraukšanas gadījumos.

## 10. Sistēmas lietotāju reģistrācija un tās atcelšanas kārtība

10.1. Jauniem darbiniekiem un akadēmiskajam personālam uzsākot darba tiesiskās attiecības uzreiz jāiepazīstas ar studiju informāciju sistēmām un saistītiem jautājumiem pirms tiek piešķirta piekļuve Koledžas Sistēmām.
10.2. Sistēmas lietotāja darba vieta tiek aprīkota ar minimāli nepieciešamajiem Sistēmas resursiem atbilstoši veicamā darba pienākumiem.
10.3. Jauna Sistēmas lietotāja pieprasījumu paraksta lietotāja tiešais vadītājs un apstiprina Sistēmas informācijas resursu turētājs atbilstoši pieejas kontroles politikai.
10.4. Katram Sistēmas lietotājam tiek piešķirts unikāls identifikators un parole, kā arī noteiktas piekļuves tiesības.
10.5. Sistēmas lietotājs ir atbildīgs par piešķirtā identifikatora un autentifikācijas rīku saglabāšanu un neizpaušanu.
10.6. Aizliegts piekļūt tiem Sistēmas resursiem, kuriem nav piešķirtas piekļuves tiesības.
10.7. Sistēmas lietotāja reģistrācija tiek atcelta:
10.7.1. Lietotājam izbeidzot darba attiecības ar Augstskolu;
10.7.2. Pēc lietotāja tiešā vadītāja pieprasījuma;
10.7.3. Sistēmas drošības prasību neievērošanas gadījumā.

**11. Sistēmas lietotāju tiesības, pienākumi, ierobežojumi un atbildība**

11.1. Sistēmas lietotājam ir tiesības saņemt konsultācijas no atbildīgā par informācijas drošības pārvaldību un Sistēmas tehnisko resursu valdītāja par sistēmas darbību un drošības prasībām.

11.2. Sistēmas lietotājam ir tiesības izmantot piešķirtos Sistēmas informācijas resursus tikai darba pienākumu veikšanai.

11.3. Sistēmas lietotājam ir pienākums nekavējoties ziņot atbildīgajai personai par informācijas drošības pārvaldību (e-pasts andris@Koledža.lv), ja:

11.3.1. Radušās aizdomas, ka autentifikācijas rīku ir uzzinājusi/ieguvusi cita persona;

11.3.2. Radušās aizdomas par novirzēm Sistēmas darbībā.

11.4. Sistēmas lietotājam ir pienākums izlasīt Sistēmas administratora sūtītos ziņojumus un laikus izpildīt norādītās darbības.

11.5. Sistēmas lietotājam ir aizliegts:

11.5.1. Izmantot Sistēmas informācijas un tehniskos resursus, lai izplatītu vai uzglabātu ar darbu nesaistītu informāciju;

11.5.2. Veikt darbības, kas nepamatoti noslogo Sistēmas informācijas un tehniskos resursus;

11.5.3. Nesankcionēti nodot Sistēmas informācijas vai tehniskos resursus trešajai personai;

11.5.4. Nesankcionēti mainīt Sistēmas konfigurāciju un iejaukties Sistēmā.

11.6. Sistēmas lietotājs ir atbildīgs par zaudējumiem, kas radušies šajos noteikumos noteikto prasību neievērošanas dēļ.

11.7. Sistēmas lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa identifikatoru un autentifikācijas rīku, kā arī par zaudējumiem, kas radušies, neievērojot informācijas drošības prasības.

11.8. Ja lietotājs vairs nav Koledžas darbinieks vai students vai viņam ir piešķirta jauna pozīcija un/vai pienākumi Augstskolā, ir jāpārskata lietotāja piekļuve un autorizācija.

**12. Nepieņemamas lietošanas prasības**

12.1. Informācija, kas ir krāpnieciska vai citādi nelikumīga vai nepiemērota, skatīšana, izveidošana vai pārsūtīšana.

12.2. Sensitīvus datus un konfidenciālus datus nedrīkst pārsūtīt nešifrētā veidā un jāpiemēro atbilstoši drošības mehānismi, ja tiek veikta to pārsūtīšana.

12.3. Lietotāju draudēšana un iebiedēšana, ieskaitot jebkuru ziņojumu, kas varētu būt iebiedēšana vai uzmākšanās, piemēram, uz dzimuma, rases, invaliditātes, reliģijas vai pārliecības, seksuālās orientācijas vai vecuma pamata.

12.4. Lietot rupju un apvainojošu valodu, lai pamudinātu naidu pret jebkuru etnisko, reliģisko vai citu minoritāšu grupu.

12.5. Veikt intelektuālā īpašuma tiesību pārkāpumus, ieskaitot autortiesības, preču zīmi, patentu, dizainu un morālās tiesības; izplatīt nevēlamu reklāmu, ko dēvē par "surogātpastu".

12.6. E -pasta ziņojumu viltošana, kas paredz, ka nāk no kāda konkrēta indivīda, bet faktiski sūtītājs ir cits.

12.7. Darbība vai bezdarbība, kas apzināti vai netīši izraisa Koledžas informācijas drošības pārkāpumu, ieskaitot, bet ne tikai:

12.7.1. Datorvīrusu vai citas ļaunprātīgas programmatūras izplatīšana;

12.7.2. Mēģinājumi piekļūt informācijai, kurai lietotājs nav autorizēts;
12.7.3. Koledžas Sistēmu izmantošana personīgā komerciālā biznesa vai tirdzniecības veikšanai;
12.7.4. Nesamērīga laika pavadīšana vietnēs, kas nav saistītas ar darbu, piemēram, sociālo mediju vietnes;
12.7.5. Neautorizēta informācijas piekļūšana, skatīšana, kopēšana, mainīšana vai iznīcināšana;
12.7.6. Iesaistīšanās darbībās, kuru mērķis ir paslēpt lietotāja identitāti;
12.7.7. Lietotāja kontu, lietotāja ID, paroļu vai citu mehānismu kopīgošana vai pārsūtīšana citiem, kas ļauj viņiem piekļūt Koledžas informācijas aktīviem;
12.7.8. Programmatūras vai aparatūras izmantošana vai neautorizēta konfigurēšana, lai tā apzināti ļautu piekļūt neautorizētiem lietotājiem un iegūt neatļautus datus;
12.7.9. Izmantot lietotāja ID, piekļuves datus, privilēģijas vai informāciju, kurai lietotājs nav pilnvarots viņu pašreizējos apstākļos.

12.8. Mēģinājums apiet vai sagraut jebkuras Sistēmas drošības mehānismus. Lietotājiem ir aizliegts izmantot jebkuru datorprogrammu vai ierīci, lai pārtvertu un/vai atšifrētu piekļuves kontroles informāciju.

12.9. Jebkura rīcība, kas var diskreditēt vai kaitēt Koledžai, tā personālam vai telpām, vai arī citādi var uzskatīt par tīši neētisku un nepieņemamu. Piemēram, šādas darbības tiks uzskatītas par šīs Politikas pārkāpumu:
12.9.1. Mūzikas, video, filmu, filmu vai citu materiālu skatīšana, lejupielāde, izplatīšana vai glabāšana, kurai lietotājam nav derīgas licences vai citu derīgu atļauju no autortiesību turētāja;
12.9.2. Pirātiskas programmatūras izplatīšana un/vai saglabāšana;
12.9.3. Neatļautas un/vai kaitīgas ierīces pievienošana Koledžas tīklam, t.i., kura nav konfigurēta, lai ievērotu Politiku un citus attiecīgus Koledžas noteikumus un vadlīnijas, kas saistītas ar informācijas drošību;
12.9.4. Tīkla piekļuves kontroles apiešana;
12.9.5. Tīkla datu plūsmas uzraudzība un/vai pārtveršana bez atļaujas;
12.9.6. Izpēte par Sistēmu drošības trūkumiem ar tādām metodēm kā portu skenēšana u.c., bez atļaujas;
12.9.7. Jebkuras ierīces pieslēgšana ar tīkla piekļuves punktiem, ieskaitot bezvadu, kuriem lietotājam nav atļaujas;
12.9.8. Ar darbu nesaistītas darbības, kas rada lielu tīkla datu plūsmu, īpaši tās, kas traucē citiem lietotājiem Sistēmu izmantošanu vai dēļ kurām rodas finansiālās izmaksas;
12.9.9. Pārmērīga resursu izmantošana, piemēram, failu krātuve, izraisot pakalpojumu atteikumu citiem;
12.9.10. CD, DVD un citu atmiņas līdzekļu izmantošana, lai kopētu nelicencētu programmatūru, mūziku utt.;
12.9.11. Citu cilvēku vietnes materiāla kopēšana bez autortiesību turētāja skaidras atļaujas;
12.9.12. Vienādranga tīkla (angl. – "*Peer-to-peer*") un saistītu programatūru izmantošana.

12.10. Koledžas Sistēmas negodprātīgas izmantošanas gadījumi būs pakļauti disciplinārajām procedūrām un atsevišķos gadījumos var būt piemērota krimināltiesiskā atbildība.

12.11. Paroles aizliegts glabāt nešifrētā veidā, brīvi pieejamā un redzamā vietā.
12.12. Ja Koledžas tīkls tiek izmantots, lai piekļūtu citam tīklam, jebkura šī tīkla pieņemamās lietošanas prasības ļaunprātīga izmantošana tiks uzskatīta par nepieņemamu Koledžas tīkla lietošanas prasību neievērošanu.
12.13. Periodiski Koledžas IT nodaļa var īstenot tehniskus pasākumus, lai uzraudzītu aktivitātes Koledžas tīklā, lai nodrošinātu šīs Politikas prasību atbilstību un veiktu pārbaudes drošības vajadzībām.

## 13. Sistēmas lietotāju atbalsta kārtība

13.1. Koledžas nodrošina lietotāja darba pienākumiem nepieciešamos Sistēmas tehniskos un informācijas resursus.
13.2. Koledža nodrošina lietotāja informēšanu par:
13.2.1. Sistēmas darbību;
13.2.2. Sistēmas darbības plānotajiem pārtraukumiem;
13.2.3. Rīcību neplānotu Sistēmas darbības pārtraukumu laikā.
13.3. Sistēmas lietotāju atbalsta kontaktinformācija (e-pasts: andris@Koledža.lv).

## 14. Sistēmas lietošanas kārtība

14.1. Piekļuve studiju informācijas Sistēmām ir iespējama tikai autorizējoties izmantojot Koledžas tīmekļa vietni (https://www.alberta-koledza.lv) savādāk veicot autorizāciju citos veidos iekārta tiks bloķēta.
14.2. Sistēmu izmanto Koledžas uzdevumu un funkciju veikšanai.
14.3. Sistēmu izmanto Koledžas darba laikā, izmantojot Koledžas piešķirtos līdzekļus.
14.4. Visas lietotāja darbības Sistēmā var tikt uzraudzītas, un iegūtie dati var tikt izmantoti darba pienākumu izpildes kontroles nodrošināšanai un vispārīgai informācijas drošības nodrošināšanai Augstskolā.

## 15. Portatīvo datoru drošība

15.1. Datus nedrīkst glabāt portatīvajā datorā uz cietā diska, bet gan tie jāglabā uz Koledžas faila serveri.
15.2. Portatīvā datora drošība:
15.2.1. Portatīvā datora sagatavošanu darbam nodrošina Koledžas IT atbalsta dienests;
15.2.2. Lietotājs nodrošina, lai portatīvie datori vai mobilās ierīces netiek atstātas bez uzraudzības, piemēram, ceļojot jāpārliecinās, ka portatīvie datori tiek glabāti droši;
15.2.3. Lietotājs nodrošina, ka portatīvie datori netiek atstāti bez uzraudzības nedrošās vietās, piemēram, sapulču telpās blakus publiskās piekļuves zonām un viesnīcu numuriem, kur citi var piekļūt. Lietotājam jāizmanto portatīvo datoru slēdzenes un/vai pametot darba telpu durvis jāslēdz;
15.2.4. Lietotājs ir informēts par to, kāds potenciāls ir oportūnistiskai vai mērķtiecīgai portatīvā datora somu zādzībai aizņemtās sabiedriskās vietās, tostarp lidostās, vilcienu stacijās, viesnīcu lobijos, izstāžu zālēs u.c., un sabiedriskajā transportā, piemēram, autobusos un vilcieniem. Ceļojot, jāizvairās izvietot portatīvos datorus vietās, kur tos varētu viegli aizmirst vai atstāt aiz muguras, piemēram, taksometra sēdekļu kabatās. Jāapzinās, ka portatīvā datora izmantošana sabiedriskās vietās, visticamāk, pievērsīs uzmanību tiem, kas atrodas tuvumā. Iespējams, ka portatīvā datora ekrānā redzamā informācija var izraisīt šīs informācijas neatļautu izpaušanu,

tāpēc konfidenciālu informāciju publiskās vietās nav ieteicams apstrādāt vai izmantot attiecīgi privātuma filtrus ekrānam;

15.2.5. Jānodrošina, ka vienmēr tiek veikti laicīgi programmatūras un operētājsistēmas atjaunojumi tiklīdz tādi ir pieejami.

**16. Mobilās ierīces drošība**

16.1. Mobilo ierīču prasībām jāietver fiziskā aizsardzība un piekļuves kontrole, kriptogrāfiskie paņēmieni (datu šifrēšana), dublējumkopijas un antivīrusu aizsardzība, kur tas tehniski ir iespējams.

16.2. Lietotājs ņem vērā labo praksi, lai iestatītu papildus drošības un konfidencialitātes iestatījumus mobilajām ierīcēm, kā, piemēram:

16.2.1. Atbloķēt mobilo ierīci ar pin kodu vai pirkstu nospiedumu vai citiem biometriskiem līdzekļiem;

16.2.2. Ja pieejams iestata "angl.- *find my phone*" funkcionalitāti un iespēju attālināti dzēst datus un bloķēt mobilo ierīci;

16.2.3. Lietotājam jāpārbauda un jāpārskata lietotņu atļaujas;

16.2.4. Reklāmu un "angl. - *ad-tracking*" reklāmu un atrašanās vietas izsekošanas izslēgšana, lai novērstu reklāmu tīklu veidošanu, pamatojoties uz to, kādas personiskās izvēles patīk un nepatīk, pamatojoties uz skatīšanu, lasīšanu vai citiem ieradumiem;

16.2.5. Tālruņa miega taimauta mazināšana/izslēgšana un automātiska bloķēšana pēc noteikta laika perioda;

16.2.6. Bloķēt bloķēšanas ekrāna paziņojumus, lai neļautu citiem redzēt personisku saturu, kāds tas ir arī ja nav zināms PIN kods mobilai ierīcei;

16.2.7. Nepieļaut nesankcionētu programmu instalēšanu: veids, kā to nodrošināt, ir lai tālrunī ir tikai verificētas instalētas programmas, nodrošinot, ka nezināmo avotu iespēja ir izslēgta; kā arī periodiski pārbaudot, vai nav programmatūras atjauninājumu;

16.2.8. Nodrošināt, ka vienmēr tiek veikti laicīgi programmatūras un operētājsistēmas atjaunojumi tiklīdz tādi ir pieejami.

**17. Atnesiet savu ierīci (angl. - "*Bring your own device*" - BYOD) prasības**

17.1. Koledža ļauj lietot personīgi piederošas ierīces pie sekojošiem nosacījumiem:

17.1.1. Visiem personīgi piederošiem portatīvajiem datoriem, darbstacijām, mobilajiem tālruņiem vai citām ierīcēm ir jābūt apstiprinātai vīrusu un spiegprogrammatūras atklāšanas/aizsardzības programmatūrai kopā ar personīgo ugunsmūra aizsardzību;

17.1.2. Iekārtām, kurām ir piekļuve Koledžas e-pastam, ir jābūt iespējotai PIN vai citam autentifikācijas drošam mehānismam;

17.1.3. Konfidenciālu informāciju drīkst glabāt tikai ierīcēs, kas ir šifrētas saskaņā ar Koledžas informācijas drošības politiku;

17.1.4. Vēlams izmantot CERT.LV DNS ugunsmūri (vairāk informācija pieejama https://dnsmuris.lv);

17.1.5. Jebkuras ierīces, kas izmantotas, lai izveidotu, glabātu vai piekļūtu konfidenciālai informācijai, zādzība vai zudums nekavējoties jāpaziņo informācijas drošības pārvaldniekam;

17.1.6. Visām ierīcēm jābūt ar atjaunotām programmatūrām un operētājsistēmas versijām;
17.1.7. "angl. - *Jail-broken*" jeb sakņotās ierīces nedrīkst izmantot, lai izveidotu savienojumu ar Koledžas informācijas resursiem.

17.2. Koledža patur tiesības anulēt personiski piederošas ierīces lietošanas tiesības gadījumā, ja lietotāji neievēro šajā Politikā noteiktās prasības.

17.3. Savu ierīču izmantošanas gadījumi ietver arī iepriekš minētās prasības mobilajās ierīcēs un portatīvā datora drošības sadaļās.

## 18. Interneta un elektroniskā pasta lietošana

18.1. Koledžas elektronisko pastu atļauts izmantot vienīgi darba un/vai studiju vajadzībām un aizliegts to norādīt kā privāto kontaktinformāciju dažādos interneta portālos vai citās publiskās vietnēs.

18.2. Lietotāji nedrīkst izmantot Koledžas e-pastu personīgajām vajadzībām vai personīgā labuma gūšanai.

18.3. Lietotāji nedrīkst lejupielādēt programmatūru no interneta vai izpildīt vai pieņemt jebkādas programmatūras vai citu kodu internetā, ja vien tas neatbilst Koledžas politikām un procedūrām.

18.4. Aizliegts atvērt no nezināmiem avotiem saņemtus e-pasta pielikumus un e-pastos norādītās interneta adrešu saites. Par šāda e-pasta saņemšanas faktu nekavējoties jāziņo IT atbalsta dienestam.

18.5. Lietotājam, saņemot e-pastu un pastāvot šaubām par iespējamu datorvīrusu, nekavējoties jāziņo IT atbalsta dienestam.

18.6. Aizliegts atkārtoti sūtīt e-pasta vēstuli, ja ir saņemts paziņojums, ka adresāts nevar saņemt sūtījumu e-pasta servera limita pārsniegšanas dēļ.

18.7. Viena e-pasta sūtījuma apjoms nedrīkst pārsniegt 20 megabaiti (turpmāk - MB).

18.8. Liela izmēra failus apmaiņai jāizmanto Koledžas failu apmaiņas servisu https://alberta-koledza.sharepoint.com.

18.9. E-pasta lietotājam, regulāri nodzēšot nevajadzīgo informāciju, jākontrolē, lai viņa pastkastes apjoms serverī nepārsniegtu 7 GB. IS administrators drīkst bloķēt lietotāja e-pasta kontu, ja pastkastes kopapjoms pārsniedz minēto apjomu.

## 19. Programatūra un informācijas sistēmas

19.1. Darba un studiju pienākumu veikšanai atļauts lietot tikai licencētu un autorizētu programmatūru. Nelicencētas vai privātai lietošanai paredzētas programmatūras uzstādīšana un lietošana uz Koledžas datoriem ir aizliegta.

19.2. Aizliegts patstāvīgi veikt programmatūru uzstādīšanu vai noņemšanu uz Koledžas iekārtām bez IT nodaļas vadītāja rakstiskas atļaujas.

## 20. Sistēmas drošības kritēriji

20.1. Sistēma ir pieejama nepārtraukti.

20.2. Nosacījumi, pie kuriem ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām:
20.2.1. Ja Sistēmas darbības atjaunošanas laiks pārsniedz pieļaujamo;
20.2.2. Ja Sistēmā konstatēts datu zudums.

## 21. Noslēguma jautājumi

21.1. Politiku pārskata vismaz reizi gadā, kā arī šādos gadījumos:

21.1.1. Ja izmaiņas Sistēmā var ietekmēt Sistēmas drošību;

21.1.2. Ja ir mainījušies vai atklāti jauni Sistēmas drošības apdraudējumi;

21.1.3. Ja pieaug Sistēmas drošības incidentu skaits vai noticis nozīmīgs Sistēmas drošības incidents.

21.2. Ja, pārskatot politiku, konstatēta atbilstoša nepieciešamība, to aktualizēt.

21.3. Ja izmaiņas Koledžas organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju.

21.4. Ja mainās procesu nosaukumi, Koledžas struktūrvienību nosaukumi, atbildīgie darbinieki, viņu amati, darba vietas adreses, telefonu numuri u.tml., ir mainījušies Koledžas iekšējie normatīvie akti, kā arī atsauces un saites uz citiem saistītajiem dokumentiem, tad tie netiek uzskatīti par dokumenta grozījumiem.

21.5. Ja tiek izdarītas būtiskas izmaiņas dokumenta saturā un tajā aprakstītajās darbībās, grozījumus apstiprina Koledžas vadība.

21.6. Atbildīgs par Politikas aktualizēšanu ir informācijas drošības pārvaldnieks.