BANKU AUGSTSKOLA

PVN Reģ. Nr. LV 90000437699, K.Valdemāra ielā 161, Rīgā, LV-1013, tālr.67360133, fakss 67320620, e-pasts: info@ba.lv, http://www.ba.lv

APSTIPRINĀTS
Banku augstskolas
Senāta 22.05.2018. sēdē,
protokols Nr.6

Vispārējā kārtība darbstaciju un elektroniskās informācijas un tehnisko resursu lietotājiem

Rīgā

Izdots saskaņā ar Augstskolu likuma 15.panta pirmo daļu un Banku augstskolas Satversmes 21.punktu

2018.gada 22.maijā Nr.1.5-2/11

I. Vispārīgie noteikumi

1. Vispārējā kārtība darbstaciju un elektroniskās informācijas un tehnisko resursu lietotājiem (turpmāk – kārtība) nosaka drošības prasības Banku augstskolas (turpmāk – augstskola) personālam, praktikantiem, kā arī pakalpojumu sniedzējiem saskaņā ar noslēgto līgumu, kuri lieto augstskolas darbstacijas (portatīvais dators vai stacionārais datorkomplekts - sistēmbloks, monitors, klaviatūra, pele),elektroniskās informācijas un tehnisko resursus (turpmāk – lietotāji).

2. To personu, kuras nav augstskolas personāls, piekļūšanai augstskolas darbstacijām, elektroniskās informācijas un tehniskajiem resursiem (turpmāk – resursi) ir atļauta tikai ar Informācijas tehnoloģiju daļas (turpmāk – IT daļa) vadītāja vai IT daļas darbinieku atļauju.

3. Augstskolas iekšējam datortīklam ir tiesības pieslēgt tikai augstskolas īpašumā, valdījumā vai lietošanā esošu datortehniku un jebkāda veida datora ārējo papildaprīkojumu (turpmāk - perifērijas iekārtas).

4. Ja kāds no augstskolas personāla vēlas izmantot privāto datoru un piekļūt augstskolas iekšējam datortīklam un resursiem, tad privātais dators tiek reģistrēts augstskolas aktīvajā direktorijā (drošības un lietotāju autentifikācijas resursā, kas nodrošina vienotu lietotāju identifikāciju dažādiem resursiem). Lietotājs ievēro lietotāja drošības politiku un viņam tiek liegta iespēja veikt jebkādas darbības ar augstskolā izmantojamajām elektroniskajām informācijas sistēmām (turpmāk – informācijas sistēmas), kas var ietekmēt vai apdraudēt augstskolas resursu drošību.

II. Lietotāju piekļuves kontrole

5. Lietotājam tiek piešķirts informācijas sistēmas lietotājvārds un parole, kā arī noteiktas piekļuves tiesības. Lietotājs ir atbildīgs par piešķirtā lietotājvārda un paroles lietošanu, saglabāšanu un neizpaušanu.

6. Lietotājs ievēro šādus paroles izveides nosacījumus:

6.1. parole sastāv no burtu un zīmju kombinācijas, bet tā nedrīkst saturēt garumzīmes un mīkstinājuma zīmes, un tās garums nedrīkst būt īsāks par astoņiem simboliem;

6.2. parole nedrīkst saturēt lietotāja vārdu un uzvārdu dažādās kombinācijās;

6.3. paroli maina vismaz reizi 180 dienās;

6.4. lietotājs ir atbildīgs par paroles nomaiņu pamatojoties uz 6.1., 6.2., 6.3.apakšpunktu. Ja, mainot paroli, lietotājam ir neskaidrības, viņš sazinās ar IT daļas darbiniekiem.

7. IT daļa nodrošina, ka uz datora tiek uzstādīts ekrānsaudzētājs ar aktivizācijas paroli, kas ieslēdzas pēc noteikta laika perioda dīkstāves.

8. Piekļuve augstskolas resursiem un lietotāja konts tiek automātiski bloķēti pēc 5 neveiksmīgiem pieslēgšanās mēģinājumiem. IT daļas darbinieki veic lietotāja konta atbloķēšanu.

9. Ja lietotājam ir nepieciešama papildu piekļuve informācijas sistēmai konkrēta darba veikšanai, lietotājs iesniedz rektoram pamatotu iesniegumu par piekļuves tiesību saņemšanu attiecīgajai informācijas sistēmai, norādot nepieciešamo piekļuves līmeni. IT daļas vadītājs piešķir piekļuves tiesības, pamatojoties uz rektora rezolūciju vai rīkojumu.

10. Personāla vadītājs nodrošina IT daļas informēšanu par lietotājiem, kuriem uzsāktas vai izbeigušās tiesiskās attiecības ar augstskolu, kā arī informācijas par lietotājiem aktualizēšanu augstskolas informatīvajā sistēmā.

11. IT daļas darbinieki, pamatojoties uz kārtības 10.punktā saņemto informāciju, izveido vai bloķē lietotāja piekļuvi augstskolas informācijas sistēmām un resursiem.

III. Lietotāju pienākumi

12. Lietotāja pienākums ir ievērot:

12.1. informācijas apstrādes, resursu un perifērijas iekārtu lietošanas drošības noteikumus un saistītās procedūras.

12.2. elektroniskās informācijas īpašnieka (personas, kas ir atbildīga par konkrētās informācijas radīšanu, izmantošanu, dzēšanu, kā arī atļauju vai liegumu pieejai elektroniskai informācijai datu ievades, skatīšanās vai labošanas režīmā) un augstskolas tehnisko resursu turētāja (darbinieka, kas nodrošina tehniskos resursus informācijas aprites nodrošināšanai tādā apmērā, kā to pieprasa elektroniskās informācijas īpašnieks) izvirzītos papildu drošības noteikumus un procedūras.

13. Lietotājs ir atbildīgs par visām darbībām, kas veiktas, izmantojot viņam piešķirtās piekļuves tiesības uz informācijas sistēmu un resursu lietošanu.

14. Lietotājam ir aizliegts izpaust informāciju, kas nodrošina pieeju augstskolas resursiem un lietotājs ir personīgi atbildīgs par tās konfidencialitāti.

15. Atstājot darbstaciju, lietotājs veic darbstacijas bloķēšanu.

16. Ja lietotājam ir nepieciešamas atjaunot pieejas datus augstskolas informācijas resursiem, viņš sazinās ar IT daļas darbiniekiem.

17. Lietotājam ir aizliegts izpaust savu piekļuves paroli citai personai, kā arī aizliegts paroles informāciju pārsūtīt, izmantojot interneta, e-pasta vai mobilo telefona sakaru operatoru sniegtos pakalpojumus.

18. Ja lietotājam ir aizdomas par to, ka viņam piešķirto piekļuves paroli ir izmantojusi kāda cita persona, viņš nekavējoties ziņo IT daļas vadītājam.

IV. Vispārējie lietošanas noteikumi

19. Lietotājs drīkst mainīt, dzēst vai pievienot elektroniskos datus, ja ir piešķirtas attiecīgās lietotāja tiesības konkrētam lietotājam.

20. Lietotājam bez IT daļas darbinieku atļaujas aizliegts piekļūt resursiem vai izmantot cita lietotāja piekļuves tiesības.

21. Gadījumā, ja neautorizētā pieeja notikusi nejauši vai kļūdas rezultātā, lietotājs nekavējoties atslēdzas no neautorizētās vietnes un informē par notikušo IT daļu.

22. Lietotājiem ir aizliegts izpaust vai nodot elektronisko informāciju ārpus augstskolas bez saņemta rektora vai IT daļas vadītāja pilnvarojuma, izņemot gadījumus, ja tas nepieciešams studiju procesa nodrošināšanai vai tiešo darba pienākumu veikšanai, nepārkāpjot Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulas (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz fiziskās personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula) (turpmāk – regula) normas.

23. Lietotājam elektronisku informāciju atļauts dzēst vai kā citādi iznīcināt ar elektroniskās informācijas resursa īpašnieka atļauju.

24. Lietotājam ir aizliegts patvaļīgi uzstādīt un lietot programmatūru. Programmatūru lietotājs drīkst uzstādīt un lietot ar IT daļas vadītāja atļauju.

25. Lietotājam ir aizliegts atinstalēt vai deaktivizēt instalētās pretvīrusu un citas drošības programmas.

26. Gadījumā, ja programmatūra nefunkcionē tā, kā paredzēts, vai arī tās darbība šķiet aizdomīga, lietotājs par to nekavējoties ziņo IT daļai.

27. Ja lietotājam ir aizdomas par drošības pārkāpumu vai datorvīrusu savā darbstacijā, viņš ievēro šādus nosacījumus:

27.1. iegaumē aizdomīgās pazīmes un paziņojumus, kas parādās uz ekrāna;

27.2. izslēdz datoru;

27.3. par notikušo incidentu nekavējoties ziņo IT daļai;

27.4. aizliegts izmantot datu nesēju, kas atradies lietotāja darbstacijā, citā augstskolas datorā;

27.5. aizliegts patstāvīgi mēģināt deaktivizēt un atinstalēt programmatūru, kas varētu būt inficēta ar datorvīrusu.

28. Lietotājs, beidzot darbu, iziet no vietnēm vai programmatūrām un izslēdz datoru, izņemot gadījumus, ja ir saņemta rekomendācija no IT daļas par pretējo, vai tas var ietekmēt augstskolas procesu nepārtrauktību.

29. Ja lietotājam ir nepieciešams pieslēgt iekārtu, kura nav augstskolas īpašumā, viņš to saskaņo ar IT daļas vadītāju.

30. Lietotājam ir aizliegts mainīt datora konfigurāciju (ieskaitot BIOS parametrus, informāciju reģistros, standarta uzstādījumus).

31. Lietotājs informāciju, kurai ir nepieciešama rezerves kopēšana, glabā uz failu servera. Pieeju failu serverim lietotājs var iegūt, sazinoties ar IT daļas darbiniekiem.

32. Katram lietotājam ir izveidota mape rezerves kopiju glabāšanai uz centrālā failu servera, pie tās var piekļūt atverot H disku, kas atrodas My Computer. Šis resurss ir pieejams 1 GB apjomā, ja to ir nepieciešams palielināt, lietotājs sazinās ar IT daļu.

33. IT daļa nodrošina rezerves kopēšanu un kopiju uzglabāšanu tai informācijai, kas atrodas uz centralizētiem failu vai datu bāzu serveriem.

34. Pieeju augstskolas iekšējiem datu serveriem lietotājam nodrošina IT daļas darbinieks saskaņā ar rektora rīkojumu vai, pamatojoties uz attiecīgā lietotāja amatu aprakstu.

35. Ja ir saņemta rektora atļauja, IT daļa nodrošina lietotājam tiešo darba pienākumu veikšanai iespēju pieslēgties augstskolas darbstacijai no citas darbstacijas ārpus augstskolas *(Remote Desktop conection).*

36. Lietotājam ir aizliegts pie darbstacijas dot fizisku piekļuvi personām, kurām nav tiesību tur atrasties.

V. Elektronisko datu nesēju glabāšanas, lietošanas un iznīcināšanas kārtība

37. Augstskolas personālam ir pienākums ievērot drošības pasākumus darbā ar tiem lietošanā nodotajiem datu nesējiem neatkarīgi no to veida.

38. Datu nesēju aizsardzības ietvaros IT daļa nodrošina augstskolas īpašumā esošu datu nesēju fizisko aizsardzību, novēršot to nesankcionētu lietošanu.

39. Darba informācijas kopēšanu uz ārējiem informācijas (datu) nesējiem (piemēram, CD vai DVD diski, vai USB zibatmiņas) augstskolas akadēmiskais un vispārējais personāls drīkst veikt vienīgi savu tiešo darba uzdevumu izpildei, nepārkāpjot Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulas (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz fiziskās personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula) normas.

40. Augstskolas akadēmiskais un vispārējais personāls nodrošina, ka datu nesēji ar ierobežotas pieejamības informāciju, tiek glabāti tādā veidā, kas padara neiespējamu tā pieejamību trešajām personām. Augstskolas akadēmiskais un vispārējais personāls ir atbildīgs par attiecīgajā datu nesējā iekļauto augstskolas pārziņā esošo fizisko personu datu drošību.

41. Augstskolas akadēmiskais un vispārējais personāls, lietojot datu nesējus, kas ietver darba informāciju, ārpus augstskolas telpām, nodrošina tādu datu nesēja glabāšanas veidu, kas padara

neiespējamu tā pieejamību trešajām personām. Augstskolas akadēmiskais un vispārējais personāls ir atbildīgs par attiecīgajā datu nesējā iekļauto augstskolas pārziņā esošo fizisko personu datu drošību.

42. Augstskolas akadēmiskajam un vispārējam personālam aizliegts datu nesējus atstāt publiski pieejamās vietās.

43. Ja augstskolas datu nesējus, kas satur ierobežotas pieejamības informāciju, ir paredzēts iznīcināt, tad to izdara tādā veidā, lai nebūtu iespējams veikt tajos esošo datu atjaunošanu.

44. Augstskolas akadēmiskais un vispārējais personās augstskolas datu nesējus, kuri satur fiziskas personas datus un kuri paredzēti iznīcināšanai, nogādā IT daļā. IT daļas darbinieki nodrošina minēto datu nesēju drošu iznīcināšanu šādā kārtībā:

44.1. CD, Blue Ray vai DVD matricas tiek iznīcinātas speciālā griezējā, sasmalcinot tos tā, ka nav iespējams atjaunot;

44.2. USB un SD atmiņu kartes atkārtotai lietošanai tiek pārrakstītas ar „0" un „1", vai - ar defektiem - tiek fiziski iznīcinātas;

44.3. datoru cietie diski (gan iekšējie, gan ārējie) tiek formatēti un pēc tam pārrakstīti ar „0" un „1" vai - ar defektiem - tiek fiziski iznīcināti.