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
Padomes 24.05.2024.
sēdē,
Protokols Nr. 5

BANKU AUGSTSKOLAS INFORMĀCIJAS TEHNOLOĢIJU DROŠĪBAS POLITIKA

Rīga

2024. gada 5. septembrī Nr.1.5-2-21

I. Vispārīgie jautājumi

1. Banku augstskolas informācijas tehnoloģiju drošības politika (turpmāk - politika) ir izstrādāta, lai nodrošinātu Banku augstskolas (turpmāk – Augstskola) informācijas tehnoloģiju, kas ir tehnoloģijas, kas paredzētas datu un informācijas apstrādei, iegūšanai, uzglabāšanai un izplatīšanai (turpmāk - IT), resursu drošību.
2. Politika nosaka pamatprincipus un vadlīnijas, kas ir jāievēro visiem Augstskolas darbiniekiem, studējošajiem, apakšuzņēmējiem un citiem sadarbības partneriem, kuriem ir piekļuve Augstskolas IT sistēmām un datiem (turpmāk – lietotāji).
3. Politika attiecas uz visiem informācijas aktīviem, ieskaitot, bet ne tikai, datoriem, tīkliem, serveriem, datu bāzēm, programmatūrām, lietojumprogrammām un datu pārraides sistēmām.
4. Politikas ievērošana ir obligāta visiem Augstskolas lietotājiem. Lai nodrošinātu efektīvu politikas ieviešanu, tiek veikta regulāra Augstskolas darbinieku apmācība, kā arī periodiska politikas pārskatīšana un atjaunināšana, ņemot vērā jaunākās IT attīstības tendences un drošības draudus.
5. Politika tiek īstenota kopā ar citām politikām, noteikumiem, rīkojumiem un vadlīnijām, kuras pieņem un ievieš Augstskola (piemēram, risku vadības politika, privātuma politika, u.c.).
6. Politikas mērķi ir:
   6.1. nodrošināt Augstskolas informācijas aktīvu aizsardzību pret nesankcionētu piekļuvi, izpaušanu, iznīcināšanu vai bojāšanu;
   6.2. identificēt un samazināt iespējamos IT drošības riskus, lai aizsargātu Augstskolu pret kiberdraudiem;
   6.3. nodrošināt, ka informācijas aktīvi ir pieejami atbilstoši akadēmiskajām, zinātniskās darbības un administratīvajām vajadzībām, kā arī nodrošināt IT sistēmu darbības nepārtrauktību;

6.4. nodrošināt augstu pieejamību un atteikum noturību IT sistēmām un procesiem, lai garantētu nepārtrauktu Augstskolas darbību traucējumu vai incidentu gadījumos, nodrošināt spēju ātri atjaunot IT sistēmas un turpināt kritiskos biznesa procesus ar minimālu pārtraukumu.
6.5. nodrošināt, ka IT drošības pasākumi atbilst visām Latvijas vai starptautisko normatīvo aktu prasībām, kas nosaka informācijas apstrādes un aizsardzības noteikumus, nozares standartus un labās prakses principus;
6.6. veicināt lietotāju izpratni un apmācību par IT drošības jautājumiem, lai radītu drošības apziņu visā Augstskolā.

II. Lietotāju pienākumi

7. Lietotājiem ir šādi pienākumi:6.1. izvēlēties drošas paroles, kas ietvert vismaz astoņus rakstzīmes. Lietotāji var izmantot lielos un mazos burtus, ciparus un speciālas rakstzīmes. Paroles lietotāji maina regulāri, vismaz ik pēc 180 dienām un nedrīkst tās koplietot ar citiem lietotājiem;
   7.1. izmantot daudzfaktoru autentifikāciju (MFA), ja tā ir pieejama, un ievērot visas Augstskolas noteiktās autentifikācijas prasības;
   7.2. nodrošināt, ka konfidenciālie dati ir aizsargāti un netiek izpausti neautorizētām personām;
   7.3. izvairīties no darbībām, kas var apdraudēt Augstskolas IT sistēmu drošību, piemēram, no aizdomīgu e-pastu atvēršanas vai neautorizētu programmatūru instalēšanas;
   7.4. nekavējoties ziņot par jebkādiem drošības incidentiem vai aizdomīgām darbībām Augstskolas noteiktajam datu aizsardzības speciālistam (ithelp@ba.lv);
   7.5. sniegt nepieciešamo palīdzību un informāciju drošības incidentu izmeklēšanas laikā;
   7.6. regulāri, bet ne retāk kā reizi gadā, apmeklēt IT drošības apmācības, ko nodrošina Augstskola;
   7.7. izmantot tikai licencētu un atļautu programmatūru, ko ir apstiprinājusi Augstskola;
   7.8. nodrošināt, ka viņu izmantotās ierīces un programmatūra ir regulāri atjauninātas ar jaunākajiem drošības ielāpiem;
   7.9. ievērot fizisko personu datu privātuma prasības un jārīkojas atbilstoši Latvijas Republikā spēkā esošajiem normatīvajiem aktiem, kas regulē fizisko personu datu aizsardzību un apstrādi;
   7.10. izmantot Augstskolas IT resursus efektīvi un atbilstoši paredzētajam mērķim, izvairoties no resursu pārmērīgas vai neatļautas izmantošanas.
8. Ja lietotāji izmanto personīgās ierīces Augstskolas datu vai sistēmu piekļuvei, tām jābūt aizsargātām ar atbilstošiem drošības pasākumiem.

III. Piekļuves kontrole

9. Piekļuve IT sistēmām un datiem tiek balstīta uz lietotāja lomu Augstskolā (studējošais, mācībspēks, vispārējais personāls, u.c.). Katrai lomai ir noteikti piekļuves līmeņi.
10. Lietotājiem piešķir tikai tādu piekļuvi, kas nepieciešama viņu darba pienākumu veikšanai, lai mazinātu drošības riskus.
11. Tiek izveidota skaidra procedūra piekļuves pieprasīšanai, apstiprināšanai un piešķiršanai.

12. Piekļuves tiesības jāizvērtē regulāri, ne retāk, kā reizi 180 dienās, lai pārliecinātos, ka tās joprojām ir nepieciešamas un atbilstošas.
13. Kad lietotāji pārtrauc darbu Augstskolā vai maina amatu, viņu piekļuves tiesības nekavējoties tiek atceltas vai pārskatītas, lai nodrošinātu, ka viņiem nav tādas piekļuves, kas nav nepieciešama viņu amata pienākumu pildīšanai.
14. Visi piekļuves mēģinājumi (gan veiksmīgi, gan neveiksmīgi) IT sistēmām tiek reģistrēti un uzglabāti piekļuves žurnālos. Atkarībā no IT sistēmas piekļuves mēģinājumi tiek uzglabāti no septiņām dienām līdz 365 dienām.
15. Piekļuves žurnāli tiek analizēti regulāri, ne retāk kā reizi 180 dienās, lai identificētu un izmeklētu aizdomīgas vai neatļautas piekļuves darbības.
16. Piekļuve telpām, kurās atrodas serveri un citi svarīgi IT resursi, tiek ierobežota un nodrošināta ar piemērotiem drošības pasākumiem, piemēram, elektroniskajām kartēm vai drošības personālu.
17. Augstskolas IT tehnika un citas ierīces tiek aizsargātas pret zādzību un nesankcionētu piekļuvi, piemēram, izmantojot slēdzamus skapjus vai drošības kabeļus.
18. Lietotājiem, kuri piekļūst Augstskolas resursiem attālināti, ir pienākums izmantot drošas metodes, piemēram, virtuālo privāto tīklu (turpmāk - VPN).
19. Lietotāju personīgās ierīces, kuras izmanto attālinātai piekļuvei, ir atbilstoši aizsargātas ar antivīrusu programmatūru, ugunsmūriem un izmantotā programmatūra ir atjaunināta līdz pēdējai pieejamai versijai, kā to ir noteicis attiecīgās programmatūras izstrādātājs.
20. Ja kādam lietotājam nepieciešama piekļuve, kas pārsniedz standarta piekļuves tiesības, ir noteikta skaidra izņēmumu apstrādes procedūra, ieskaitot piekļuves pieprasījuma dokumentēšanu, apstiprināšanu un monitoringu.

IV. Datu aizsardzība

21. Datu aizsardzība ir kritisks IT drošības aspekts, kas ietver pasākumus un procedūras, lai nodrošinātu datu konfidencialitāti, integritāti un pieejamību.
22. Datus klasificē pēc to jutīguma un nozīmības, piemēram, publiski, iekšēji, konfidenciāli un stingri konfidenciāli.
23. Augstskola izstrādā skaidrus kritērijus, lai noteiktu, kā dati tiek klasificēti katrā līmenī, balstoties uz to iespējamo ietekmi, ja tie tiek izpausti vai bojāti.
24. Visi jutīgie dati, kas tiek pārraidīti tīklā (piemēram, e-pasti, failu pārsūtīšana), tiek šifrēti, izmantojot drošus protokolus, piemēram, TLS (Transport Layer Security).
25. Augstskola nodrošina, ka:
    25.1. tikai autorizēti lietotāji var piekļūt jutīgiem datiem, izmantojot drošas autentifikācijas metodes un atbilstošas piekļuves tiesības;
    25.2. visi kritiskie dati tiek regulāri dublēti, lai novērstu datu zudumu gadījumos, kad notiek sistēmas kļūme vai cits incidents.
26. Regulāri tiek pārbaudītas rezerves kopijas, lai pārliecinātos, ka tās ir derīgas un ka datus var atjaunot nepieciešamības gadījumā.
27. Augstskolā lieto kontroles summas (Cryptographic checksum) un heša vērtības (Hash value), lai pārbaudītu datu integritāti un nodrošinātu, ka dati nav mainīti vai bojāti.
28. Tiek nodrošina datu pieejamība, izmantojot redundances un augstas pieejamības risinājumus, piemēram, klasterēšanu un failover sistēmas.

29. Regulāri tiek pārbaudītas un uzturētas datu glabāšanas sistēmas, lai nodrošinātu to nepārtrauktu darbību un pieejamību.
30. Augstskolā tiek izveidotas procedūras drošības incidentu noteikšanai un ziņošanai, lai nodrošinātu ātru reaģēšanu un problēmu risināšanu.
31. Visus drošības incidentus reģistrē un analizē, lai identificētu cēloņus un novērstu līdzīgus incidentus nākotnē.
32. Augstskola nodrošina, ka visi jutīgie dati tiek droši dzēsti, kad tie vairs nav nepieciešami, izmantojot drošas datu dzēšanas metodes.
33. Datu nesēji, kas satur jutīgus datus, ja tie vairs nav izmantojami, tiek iznīcināti fiziski, piemēram, izmantojot smalcināšanu vai sadedzināšanu.
34. Augstskola nodrošina atbilstību Latvijas Republikā spēkā esošo normatīvo aktu prasībām, kas nosaka informācijas apstrādes un aizsardzības noteikumus.
35. Augstskolā tiek veikti regulāri datu aizsardzības auditi, lai pārliecinātos, ka tiek ievērotas visas datu aizsardzības prasības un šī politika.
36. Augstskola nodrošina regulāras apmācības par datu aizsardzību visiem lietotājiem, lai veicinātu izpratni par drošības praksi un atbildību.

V. Tīkla drošība

37. Tīkla drošība ietver tehnoloģijas, politikas un procedūras, lai aizsargātu Augstskolas tīkla infrastruktūru no nesankcionētas piekļuves, ļaunprātīgiem uzbrukumiem un datu noplūdes.
38. Lai nodrošinātu Augstskolas tīkla drošību, nepieciešams:
    38.1. uzstādīt ugunsmūri, lai aizsargātu tīkla perimetru un kontrolētu ienākošo un izejošo datu plūsmu, balstoties uz definētiem drošības noteikumiem;
    38.2. izmantot iekšējo tīkla tehniku, tai skaitā ugunsmūri, VLAN (Virtual Local Area Networks), lai segmentētu tīklu un aizsargātu kritiskos resursus no iekšējiem draudiem;
    38.3. izmantot IDS (Intrusion detection systems) un IPS (Intrusion prevention systems), lai uzraudzītu, ierobežotu tīklā notiekošās darbības un noteiktu aizdomīgas darbības vai drošības pārkāpumus;
    38.4. nodrošināt, ka attālinātiem lietotājiem piekļuve Augstskolas tīklam ir droša, izmantojot VPN;
    38.5. nodrošināt, ka visi VPN lietotāji tiek autentificēti un autorizēti, izmantojot drošus mehānismus;
    38.6. regulāri analizēt tīkla trafiku, lai identificētu anomālijas un potenciālus drošības draudus;
    38.7. uzglabāt un pārvaldīt tīkla žurnālfailus, lai nodrošinātu efektīvu drošības incidentu izmeklēšanu un auditu;
    38.8. nodrošināt, ka visas tīkla iekārtas (maršrutētāji, ugunsmūri, u.c.) tiek regulāri atjauninātas ar jaunākajiem drošības ielāpiem un programmatūras versijām;
    38.9. izmantot automatizētus rīkus, lai pārvaldītu un izvietotu drošības atjauninājumus visā tīkla infrastruktūrā;
    38.10. nodrošināt, ka tīkla infrastruktūra ir aizsargāta pret nesankcionētām izmaiņām, izmantojot autentifikācijas mehānismus;
    38.11. nodrošināt, ka visi bezvadu tīkli izmanto spēcīgas šifrēšanas metodes;
    38.12. segmentēt publiskos un privātos bezvadu tīklus, lai ierobežotu piekļuvi kritiskiem resursiem;

38.13. izmantot DLP (Data loss prevention) risinājumus, lai monitorētu un kontrolētu sensitīvu datu plūsmu tīklā, novēršot datu noplūdi;
38.14. izstrādāt un īstenot tīkla drošības incidentu reaģēšanas plānu, lai ātri un efektīvi reaģētu uz drošības incidentiem;
38.15. izveidot un regulāri pārbaudīt tīkla atkopšanas procedūras, lai nodrošinātu nepārtrauktu darbību pēc drošības incidentiem;
38.16. nodrošināt apmācības par tīkla drošību lietotājiem, lai veicinātu izpratni par tīkla drošību un kiberhigēnu;
38.17. veikt pikšķerēšanas simulācijas un citus kiberuzbrukumu testus, lai uzlabotu tīkla drošību, lietotāju spēju atpazīt un reaģēt uz draudiem.

VI. Drošības incidentu vadība

39. Drošības incidentu vadība ir nepieciešama, lai ātri un efektīvi reaģētu uz drošības incidentiem, mazinātu to ietekmi un novērstu līdzīgus gadījumus nākotnē.
40. Lai nodrošinātu efektīvu drošības incidentu vadību, nepieciešams:
40.1. nepārtraukti uzraudzīt tīkla trafiku, sistēmu darbību un lietotāju aktivitātes, izmantojot dažādus monitoringa rīkus;
40.2. lietot uzvedības analīzes un mašīnmācīšanās metodes, lai identificētu anomālijas un aizdomīgas darbības, kas varētu norādīt uz drošības incidentu;
40.3. klasificēt drošības incidentus pēc to veida (piemēram, vīrusi, datu noplūde, DDoS uzbrukumi) un to ietekmes;
40.4. novērtēt drošības incidentu ietekmi, lai noteiktu to prioritāti un nepieciešamo reaģēšanas līmeni;
40.5. noteikt IT drošības un datu aizsardzības speciālistu;
40.6. izveidot procedūru drošības incidentu ziņošanai, kas ietver kontaktinformāciju, ziņošanas kanālus un nepieciešamo informāciju, ko jāsniedz par attiecīgo drošības incidentu;
40.7. savākt visus pieejamos datus un žurnālfailus, kas varētu palīdzēt izmeklēšanā, piemēram, tīkla trafika žurnālus, sistēmas žurnālus;
40.8. veikt ātrus pasākumus, lai apturētu drošības incidentu un minimizētu tā sekas, piemēram, atslēgt skartos kontus, izolēt inficētās sistēmas vai bloķēt ļaunprātīgus IP (Internet protocol) adreses;
40.9. izstrādāt un ieviest ilgtermiņa risinājumus, lai novērstu līdzīgu drošības incidentu atkārtošanos, piemēram, veikt programmatūras atjauninājumus, konfigurācijas izmaiņas un ugunsmūra politiku uzlabošanu;
40.10. uzturēt detalizētu drošības incidentu žurnālu, kurā tiek reģistrēti visi drošības incidenti atkarībā no noteiktā nozīmīguma līmeņa vai ietekmes uz Augstskolas IT sistēmām, veiktajām darbībām, pieņemtajiem lēmumiem un rezultātiem;
40.11. atjaunot skartās sistēmas un pakalpojumus, nodrošinot, ka tās atbilst drošības prasībām;
40.12. atjaunot zaudētos vai bojātos datus no rezerves kopijām, nodrošinot datu integritāti un pieejamību;
40.13. pēc drošības incidenta pilnīgas atrisināšanas veikt analīzi, lai izvērtētu reaģēšanas efektivitāti, identificētu nepilnības un izstrādātu uzlabojumus;
40.14. nodrošināt regulāras apmācības IT drošības un datu aizsardzības speciālistam, lai uzlabotu prasmes un zināšanas.

VII. IT sistēmu un programmatūras izmantošana

41. IT sistēmu droša izmantošana Augstskolas IT infrastruktūrā ir nepieciešama, lai aizsargātu IT sistēmas pret drošības draudiem, uzturētu IT sistēmu integritāti un nodrošinātu datu aizsardzību.
42. Lai nodrošinātu IT sistēmu drošu izmantošanu, nepieciešams:
    42.1. nodrošināt, ka visa programmatūra tiek iegūta tikai no oficiāliem un uzticamiem avotiem, lai izvairītos no ļaunprātīgas programmatūras;
    42.2. izveidot un ievērot stingras programmatūras instalācijas procedūras, kuras ietver lietotāju tiesību pārbaudi un programmatūras pārbaudi pirms instalācijas;
    42.3. nodrošināt, ka visas IT sistēmas, programmatūra un operētājsistēmas tiek regulāri atjauninātas ar jaunākajiem drošības ielāpiem;
    42.4. lietot automatizētus rīkus, lai efektīvi pārvaldītu atjauninājumus;
    42.5. regulāri pārbaudīt un auditēt sistēmu konfigurācijas, lai nodrošinātu, ka tās atbilst drošības prasībām un nav notikušas nesankcionētas izmaiņas;
    42.6. veikt regulārus sistēmu un programmatūras ievainojamību skenējumus, lai identificētu un novērstu potenciālus drošības trūkumus;
    42.7. lietot automatizētus ielāpu pārvaldības (Patch management) rīkus, lai ātri reaģētu uz identificētām ievainojamībām un instalētu nepieciešamos drošības ielāpus;
    42.8. nepārtraukti uzraudzīt sistēmu darbību un lietotāju aktivitātes, lai savlaicīgi identificētu un reaģētu uz potenciālajiem drošības incidentiem;
    42.9. pārbaudīt, vai visas izmantotās programmatūras un sistēmas ir savstarpēji saderīgas un atbilst Augstskolas drošības standartiem;
    42.10. veikt regulārus iekšējos un ārējos drošības auditus, lai pārbaudītu, vai Augstskolas IT sistēmas un izmantotās programmatūras nav pakļautas drošības riskiem;
    42.11. izvēlēties mākoņpakalpojumu sniedzējus, kas atbilst Augstskolas drošības prasībām un attiecīgais pakalpojuma sniedzējs ir sertificēts atbilstoši starptautiskiem drošības standartiem (piemēram, ISO/IEC 27001);
    42.12. ja ir iespējams, lietot spēcīgas autentifikācijas metodes, piemēram, daudzfaktoru autentifikāciju (MFA), lai piekļūtu mākoņpakalpojumiem;
    42.13. izmantojot mākoņpakalpojumus, izveidot lomu balstītu piekļuves kontroli, lai ierobežotu piekļuvi datiem un resursiem, balstoties uz lietotāja darba pienākumiem;
    42.14. nodrošināt, ka lietojot mākoņpakalpojumus, visi dati tiek šifrēti gan pārsūtīšanas laikā, gan uzglabāšanas laikā.

VIII. Noslēguma noteikumi

43. Augstskolas noteiktais datu aizsardzības speciālists:
    43.1. regulāri (vismaz reizi gadā, stājoties spēkā jaunām normatīvo aktu prasībām stāšanās spēkā vai iestājoties būtiskiem drošības incidentiem) pārskata un aktualizē IT drošības politiku, lai nodrošinātu pastāvīgu atbilstību un efektivitāti;
    43.2. analizē iepriekšējo periodu drošības incidentus, ievainojamības un riskus, lai novērtētu, vai pašreizējā politika ir bijusi efektīva;
    43.3. analizē jaunākās kiberdrošības tendences un draudus, lai identificētu, vai politikā ir jāiekļauj jauni drošības pasākumi;

43.4. organizē apmācības, lai izskaidrotu politikas izmaiņas un nodrošinātu, ka lietotāji saprot un ievēro jaunos drošības pasākumus;
43.5. regulāri uzrauga, vai politika tiek ievērota, un veic nepieciešamos pasākumus, lai nodrošinātu atbilstību.

44. Augstskola nodrošina lietotāju iepazīstināšanu ar politiku Augstskolā noteiktajā kārtībā. Politika ir pieejama Augstskolas mājaslapā.

Padomes priekšsēdētājs M. Bičevskis