Apstiprināta
ar LBTU Padomes 10.02.2023. Lēmumu Nr. 16
(Protokols Nr. 13)

Latvijas Biozinātņu un tehnoloģiju universitātes Informācijas un komunikāciju tehnoloģiju drošības politika

I. Vispārīgie jautājumi

1. Informācijas un komunikāciju tehnoloģiju drošības politika (turpmāk – Drošības politika) ir dokuments, kas nosaka Latvijas Biozinātņu un tehnoloģiju universitātes (turpmāk – LBTU) informācijas tehnoloģiju drošības galvenos pamatprincipus, informācijas sistēmu organizatoriskos pasākumus un prasības tās uzturēšanai, veidojot pamatu vienotai informācijas un komunikāciju tehnoloģiju (turpmāk – IKT) drošības pārvaldībai LBTU.
2. Drošības politika attiecas uz LBTU pārvaldībā esošiem IKT resursiem, un ir saistoša visiem par IKT pārvaldību atbildīgajiem darbiniekiem un to lietotājiem, kā arī tiem ārpakalpojumu sniedzējiem, kuri LBTU sniedz ar IKT saistītus pakalpojumus.
3. Drošības politika ir balstīta uz Ministru kabineta 28.07.2015 noteikumiem Nr.442 "Kārtība, kā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" un citiem normatīvajiem aktiem, tos integrējot LBTU procesu darbības specifikā.
4. Drošības politiku izstrādā, aktualizē un pārskata LBTU IT sistēmu drošības pārvaldnieks, un apstiprina LBTU Padome.

II. Termini

5. Drošības politikā lietotie termini:
   5.1. **informācijas tehnoloģijas (IT)** – tehnoloģijas, kuras tām paredzēto uzdevumu izpildei veic informācijas elektronisko apstrādi, tai skaitā izveidošanu, dzēšanu, glabāšanu, attēlošanu vai pārsūtīšanu;
   5.2. **IT sistēmu drošības pārvaldnieks** – par informācijas sistēmu drošību atbildīgais LBTU darbinieks;
   5.3. **Informācijas sistēma (IS)** – datu ievadīšanas, uzglabāšanas un apstrādes sistēma, kas paredz lietotāju pieeju tajā glabātajiem datiem vai informācijai;
   5.4. **informācijas resursi** – IS piederoši sistēmas faili, datu bāzes, arhīvi, datu faili u.c. informācija, kas satur sistēmā glabājamo, apstrādājamo un informācijas sistēmas lietotājiem pieejamo informāciju;
   5.5. **personas dati** – jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu;
   5.6. **informācijas resursu turētājs** – persona vai iestāde, kas organizē un vada informācijas sistēmas darbību;
   5.7. **tehnisko resursu turētājs** – persona vai iestāde, kas uztur informācijas sistēmas informācijas un tehnisko resursu funkcionalitāti;
   5.8. **lietotājs** – persona, kurai ir darba tiesiskās attiecības ar LBTU vai cits tiesisks pamats, kas paredz lietotāja tiesību piešķiršanu darbam ar LBTU pārvaldībā esošām informācijas sistēmām;
   5.9. **lietojuma administrators** – persona, kura veic IS administrēšanu saskaņā ar IS pārvaldību atbildīgo personu norādījumiem, IS tehniskajām un drošības prasībām;
   5.10. **loģiskā aizsardzība** – datu vai informācijas resursu aizsardzība, kuru realizē ar

programmatūras līdzekļiem, identificējot informācijas sistēmas lietotāju, pārbaudot viņa pilnvaru atbilstību attiecīgajām darbībām informācijas sistēmā, pasargājot informāciju no tīšas vai nejaušas maiņas vai dzēšanas;

5.11. **fiziskā aizsardzība** – tehnisko resursu aizsardzība pret fiziskas iedarbības radītu informācijas sistēmas apdraudējumu (piemēram, ugunsgrēks, plūdi, sprieguma pazemināšanās vai pārspriegums enerģijas pievades tīklā, tehnisko resursu zādzība, ekspluatācijas noteikumiem neatbilstošs mitrums, gaisa temperatūra);

5.12. **drošības incidents** – notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas resursu integritāte, pieejamība vai konfidencialitāte;

5.13. **tehniskie resursi** – serveri, tīkla aparatūra, darba stacijas, datu nesēji, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei, glabāšanai un citu funkciju veikšanai.

5.14. **mākoņdatošana** – datu glabāšana, serveru resursu vai programmatūras lietošana, kas atrodas uz citai iestādei piederošiem IKT resursiem un to nodrošina kā pakalpojumu.

III. Drošības politikas mērķis un pamatnostādnes

6. Drošības politikas mērķis ir nodrošināt tādu IKT vidi, lai LBTU informācijas un tehniskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības riskiem, vienlaikus nodrošinot LBTU informācijas integritāti, konfidencialitāti, pieejamību un kvalitatīvu darbību atbilstoši normatīvajos aktos noteiktajām funkcijām.
7. Drošības politikas pamatnostādnes reglamentē LBTU darbības pamatprincipus, prasību un pasākumu kopumu vienotas un sistematizētas pieejas izveidei, lai:
   7.1. apliecinātu LBTU apņemšanos nodrošināt informācijas un tehnisko resursu drošu pārvaldību;
   7.2. nodrošinātu vienotu pieeju IKT drošības jautājumu risināšanā LBTU;
   7.3. veidotu LBTU darbinieku un studējošo izpratni par IKT drošības jautājumiem;
   7.4. būtu par pamatu IS drošības procedūru, instrukciju un citu nepieciešamo iekšējo normatīvo aktu izstrādē un ieviešanā;
   7.5. noteiktu galvenos informācijas drošības pārvaldības principus, definētu lomas, pienākumus un IS drošības atbildību.

IV. Drošības politikas īstenošanas pamatprincipi

8. LBTU pastāvīgi tiek pilnveidots dokumentu un pasākumu kopums, kas nodrošina Drošības politikas mērķa sasniegšanu.
9. LBTU tiek nodrošināta Drošības politikas īstenošanas koordinēšana un pārraudzīšana.
10. IKT drošības procesu īstenošanas pasākumi, kas nav konkretizēti Drošības politikā, ir nosakāmi ar rektora rīkojumu vai citiem normatīvajiem aktiem.
11. Ja LBTU studējošais vai darbinieks neievēro Drošības politikas noteiktos principus vai citas IKT drošības reglamentējošās prasības, rektors var šo personu disciplināri sodīt vai piemērot citus normatīvajos aktos paredzētus ietekmēšanas līdzekļus.

V. Atbilstība normatīvajiem aktiem

12. Informācijas drošības pasākumu organizēšanu un iekšējo normatīvo aktu izstrādi, papildināšanu un atjaunošanu LBTU veic saskaņā ar spēkā esošajiem normatīvajiem aktiem.
13. IT sistēmu drošības pārvaldnieks organizē IKT drošības dokumentācijas atbilstības normatīvo aktu prasībām pārskatīšanu un regulāras IKT drošības pasākumu atbilstības pārbaudes.

14. Ja pārbaužu laikā tiek konstatēti trūkumi, tad IT sistēmu drošības pārvaldnieks organizē pasākumus to novēršanai.

VI. Drošības organizācija

15. Par Drošības politikas ieviešanu LBTU kopumā ir atbildīgs rektors, kā arī LBTU darbinieki savu pilnvaru ietvaros, kas noteiktas amata aprakstos, darba līgumos un spēkā esošajos normatīvajos aktos.
16. IS drošības pārvaldību realizē, nosakot katras informācijas apritē iesaistītās personas lomu IS drošības uzturēšanā un nosakot LBTU iekšējos normatīvajos aktos nosacījumus un prasības IS drošības uzturēšanai.
17. LBTU noteiktas šādas par IS drošības pārvaldību atbildīgo personu lomas:
    17.1. informācijas resursu turētājs;
    17.2. tehnisko resursu turētājs;
    17.3. lietojuma administrators;
    17.4. IS lietotājs.
18. Ar rektora rīkojumu tiek noteikti atbildīgie informācijas un tehnisko resursu turētāji un lietojuma administratori.

VII. IT sistēmu drošības pārvaldnieka pienākumi

19. IT sistēmu drošības pārvaldnieka galvenie pienākumi ir:
    19.1. izstrādāt un uzturēt nepieciešamos LBTU iekšējos IKT drošību reglamentējošos dokumentus;
    19.2. kontrolēt IKT drošības prasību ieviešanu un ievērošanu;
    19.3. reģistrēt konstatētos IKT drošības incidentus un risināt ar to saistītās problēmas;
    19.4. uzturēt LBTU pārvaldībā esošo IKT reģistru;
    19.5. sadarbojoties ar IS pārvaldību atbildīgajām personām, identificēt un klasificēt LBTU pārvaldībā esošās IS, kā arī veikt tām IS drošības risku analīzi;
    19.6. sagatavot IS risku pārvaldības plānu;
    19.7. informēt un konsultēt LBTU studējošos un darbiniekus IKT drošības jautājumos;
    19.8. IKT drošības draudu novēršanā sadarboties ar tiesībsargājošām iestādēm amatu aprakstā noteikto pilnvaru ietvaros;
    19.9. izvērtēt mākoņdatošanas pakalpojuma nodrošinātāja realizētos IKT resursu tehnoloģiskos un organizatoriskos pasākumus, kā arī atbilstību personas datu aizsardzības regulējošajiem normatīvajiem aktiem gadījumos, kad tādi tiek ieviesti LBTU.

VIII. Informācijas resursu turētāja pienākumi

20. Informācijas resursu turētāja pienākumi ir:
    20.1. sadarbojoties ar IT sistēmu drošības pārvaldnieku, klasificēt savā pārziņā esošos IS informācijas resursus;
    20.2. sadarbojoties ar IT sistēmu drošības pārvaldnieku un attiecīgo tehnisko resursu turētāju, piedalīties savā pārziņā esošās IS risku analīzes veikšanā;
    20.3. noteikt IS un informācijas resursu lietošanas kārtību un lemt par IS lietotāju pieejas tiesību piešķiršanu un anulēšanu;
    20.4. noteikt informācijas resursu drošības prasības, kas nav pretrunā ar normatīvajiem aktiem;
    20.5. sadarboties ar tehnisko resursu turētāju un IT sistēmu drošības pārvaldnieku IS organizatoriskajos, funkcionalitātes un drošības jautājumos.

IX. Tehnisko resursu turētāja pienākumi un tiesības

21. Tehnisko resursu turētāja pienākumi ir:
    21.1. nodrošināt tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus;
    21.2. veikt regulāras tehnisko resursu darbības pārbaudes, apkopes un programmatūras atjaunināšanu;
    21.3. nodrošināt tehnisko resursu ekspluatāciju atbilstoši ražotāja noteiktajām prasībām;
    21.4. pārraudzīt un identificēt drošības apdraudējumus;
    21.5. ziņot par drošības incidentiem IT sistēmu drošības pārvaldniekam un informācijas resursu turētājam, kā arī veikt šo incidentu novēršanu;
    21.6. veikt IS datu rezerves kopēšanu un tās pārbaudi;
    21.7. nodrošināt noklusēto paroļu nomaiņu tehniskajiem resursiem;
    21.8. nodrošināt IS un tehnisko resursu atjaunošanas procedūras, ja tehniskie resursi ir bojāti un IS funkcionēšana ir traucēta vai neiespējama;
    21.9. atslēgt datortīkla pakalpojumus, kas netiek izmantoti IS darbības nodrošināšanai;
    21.10. sadarboties ar informācijas resursu turētāju un IT sistēmu drošības pārvaldnieku:
        21.10.1. IS funkcionalitātes un drošības jautājumos;
        21.10.2. lai īstenotu prasības par informācijas resursu aizsardzību un piekļūšanu tiem;
        21.10.3. piedalīties IS risku analīzē, noteikt ar tehniskajiem resursiem saistītos IS apdraudējumus, kā arī novērtēt šo apdraudējumu īstenošanās varbūtību un ietekmi;
22. Tehnisko resursu turētājam ir tiesības:
    22.1. atslēgt tehniskos resursus, lai veiktu to uzturēšanas darbus vai tehniskās infrastruktūras uzlabošanu, brīdinot IS lietotājus, ja plānotās darbības ietekmēs IS darbību;
    22.2. bloķēt IS lietotāja kontu, liedzot pieeju informācijas resursiem, ja ir iemesli, kas var apdraudēt IS drošību, kā arī gadījumos, kad IS lietotāja piekļuves dati (lietotājvārds un parole) ir kļuvuši zināmi trešajām personām. Par veikto darbību un tās iemesliem tehnisko resursu turētājs ziņo IT sistēmu drošības pārvaldniekam.

X. Lietojuma administratora pienākumi

23. Lietojuma administratora pienākumos ietilpst:
    23.1. veikt konkrētās IS lokālā administratora funkciju, t.sk., administrēt IS parametrus un pārvaldīt tās lietotājus;
    23.2. sadarboties un konsultēties ar ārējo sistēmas izstrādātāju/uzturētāju;
    23.3. veikt IS lietotāju administrēšanu saskaņā ar informācijas resursu turētāja noteikto kārtību un nodrošināt atbalsta funkciju;
    23.4. analizēt IS veiktspēju un sniegt priekšlikumus attiecīgajam informācijas resursu turētājam par sistēmas uzlabošanas iespējām;
    23.5. sadarboties ar IT sistēmu drošības pārvaldnieku IS drošības jautājumos.
24. Rektors lietojuma administratora pienākumus var uzdot pildīt arī tehnisko resursu turētājam.

XI. IS lietotāja pienākumi

25. IS lietotāja pienākumos ietilpst IS drošības principu ievērošana, kas noteiktas Drošības politikā un citos LBTU iekšējos normatīvajos aktos.
26. IS lietotājam ir jāiepazīstas ar saistošajiem IS reglamentējošiem dokumentiem, stājoties līguma attiecībās ar LBTU vai iegūstot piekļuvi uz cita tiesiska pamata, ja personai ir nepieciešams piekļūt pie LBTU pārvaldībā esošajām IS.

XII. IS klasifikācija

27. IS klasifikācijas mērķis ir apzināt un klasificēt LBTU pārvaldībā esošās IS, iedalot tās divās grupās:
    27.1. pamata drošības IS;
    27.2. paaugstinātas drošības IS.
28. IS klasifikāciju veic informācijas resursu turētājs un IT sistēmu drošības pārvaldnieks, pēc nepieciešamības pieaicinot tehnisko resursu turētāju vai citu LBTU darbinieku atbilstoši tā kompetencē esošajiem darbības jautājumiem.
29. IS tiek klasificētas, vērtējot tās pēc informācijas resursu integritātes, konfidencialitātes un pieejamības nozīmīguma.
30. LBTU pārvaldībā esošās IS uzskaita un klasificē IS reģistrā.
31. Pasākumus un metodes IS aizsardzībai LBTU nosaka pēc piešķirtajām IS klasifikācijas grupām.
32. IS klasifikācijas metodika tiek noteikta LBTU IKT drošības reglamentējošos normatīvajos aktos.

XIII. Risku pārvaldība

33. Plānojot risku pārvaldīšanas pasākumus, IT sistēmu drošības pārvaldnieks, sadarbojoties ar IS pārvaldību atbildīgajām personām, veic IS risku analīzi.
34. Risku analīzes mērķis ir novērtēt:
    34.1. IS apdraudējuma īstenošanās varbūtību, kur IS apdraudējums ir ar nodomu, vai aiz neuzmanības izdarīta darbība, vai bezdarbība, vai iespējams notikums, kas var izraisīt informācijas dzēšanu, noklusēšanu, informācijas resursu vai tehnisko resursu maiņu, bojāšanu vai informācijas nonākšanu personu rīcībā, kuras nav tam pilnvarotas;
    34.2. iespējamo kaitējumu informācijas resursu turētājam vai LBTU, ja nav nodrošināta pietiekama IS drošība.
35. Risku analīzi regulāri (ne retāk kā reizi gadā) veic visām klasificētajām paaugstinātas drošības IS, kā arī katram jaunam ar IS saistītam projektam un IS, kurām veiktas izmaiņas, kas var būtiski ietekmēt to drošību. Analizējot riskus, jāņem vērā aktuālākā situācija attiecībā uz IS aizsardzības pasākumiem.
36. Saskaņā ar risku analīzes rezultātiem tiek sagatavots risku pārvaldības plāns par drošības pasākumu ieviešanu.
37. Risku analīzi veic, lietojot risku analīzes metodiku, kas ir noteikta LBTU IKT drošības reglamentējošos normatīvajos aktos.

XIV. Fiziskā aizsardzība

38. IS darbības nodrošināšanas tehniskie resursi tiek izvietoti ierobežotas pieejamības telpās. Pieeja šādām telpām ir tiem LBTU darbiniekiem, kuriem tā ir nepieciešama tiešo amata pienākumu veikšanai.
39. Nozīmīgajiem IKT tehnisko resursu nepārtrauktas darbības uzturēšanai izmanto nepārtrauktās barošanas ierīces.
40. LBTU tiek nodrošināta tehnisko un informācijas resursu ekspluatācijas apstākļu atbilstību šo resursu ražotāju noteiktajām ekspluatācijas un uzglabāšanas noteikumiem.
41. Fiziskās aizsardzības pasākumi tiek konkretizēti LBTU IKT drošības reglamentējošos normatīvajos aktos.

XV. IKT pārvaldība

42. IKT pārvaldību īsteno, izmantojot gan tehniskus līdzekļus, gan organizatoriskus risinājumus, nodrošinot informācijas un tehnisko resursu drošību, saskaņā ar funkcionālajām vajadzībām un atbildīgo personu norādēm.
43. IKT aizsardzībai pret kaitīgām datorprogrammām izmanto speciālu programmatūru to atklāšanai, neitralizēšanai un iznīcināšanai, kā arī par IKT drošības jautājumiem izglītojot lietotājus.
44. LBTU pārvaldībā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos IS un citu darba pienākumu pildīšanai, tiek nodrošināta pretvīrusu funkcionalitāte.
45. Lai mazinātu riskus, atsevišķām IS vai tās funkcijām tiek ierobežota pieejamība, atļaujot piekļuvi tikai no LBTU pārvaldībā esošajām galalietotāju iekārtām vai LBTU datortīkla.
46. Informācijas apmaiņu ar valsts iestādēm un organizācijām nodrošina saskaņā ar normatīvo aktu prasībām, apzinoties un samazinot riskus, kas rodas, pārsūtot vai transportējot konfidenciālu informāciju.
47. Informācijas resursu apstrāde tiek veikta, lai izpildītu LBTU noteiktos datu apstrādes mērķus.
48. Informācijas resursu apstrādi veic tie darbinieki, kuri ir tiesīgi to veikt saskaņā ar to tiešajiem darba pienākumiem.
49. IS tiek nodrošināta auditācijas pierakstu veidošana, uzglabāšana un pārraudzība, lai konstatētu neautorizētās aktivitātes vai IS apdraudējuma tuvošanos.
50. Pēc lietotāja saistību izbeigšanas ar LBTU, lietotāja personas dati tiek dzēsti no informācijas resursiem, ja to dzēšana nav pretrunā ar spēkā esošajiem normatīvajiem aktiem.
51. LBTU tiek nodrošināts, ka jebkura piekļuve pie LBTU pārvaldībā esošajām IS ir izsekojama līdz konkrētam lietotāja kontam un/vai interneta protokola adresei.
52. IS tiek uzlikti visi būtiskie pieejamie programmatūras atjauninājumi, iepriekš izvērtējot to nepieciešamību un tehnisko atbalstu.
53. LBTU pārvaldībā esošajiem tehniskajiem resursiem neizmanto noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles. Piekļūšana to administrēšanas funkciju veikšanai ir iespējama tikai no konkrēta datu tīkla.
54. LBTU tiek nodrošināts, ka ierobežotas pieejamības informāciju internetā pārsūta tikai šifrētā veidā.
55. IKT pārvaldības pasākumi tiek konkretizēti LBTU IKT drošības reglamentējošos normatīvajos aktos.

XVI. IS ieviešana un uzturēšana

56. Pirms LBTU izstrādā, ievieš vai uzsāk iepirkumu par jaunu IS izstrādi, LBTU definē un apstiprina IS drošības prasības saskaņā ar Drošības politiku un nodrošina, ka IS tās tiek realizētas.
57. LBTU nodrošina šādas IS pamata drošības prasības:
    57.1. lietotāji, kas veic sistēmas administrēšanas darbu, izmanto īpašus lietotāju kontus, kas netiek izmantoti ikdienas darbību veikšanai;
    57.2. lietotāja konts ir saistīts ar konkrētu fizisko personu;
    57.3. lai izvairītos no kļūdām, datu zudumiem, neautorizētām izmaiņām un informācijas ļaunprātīgas izmantošanas, IS ir ieviestas kontroles, kuru ietvaros veic datu pārbaudi ievades, apstrādes un izvades procesos;
    57.4. lietotāja paroles garums nav mazāks par deviņiem simboliem un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu vai speciālu simbolu;
    57.5. lietotāja parole ievadīšanas brīdī lietotājam netiek pilnībā attēlota;

57.6. lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir lietojama vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;
57.7. lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros, izņemot šo noteikumu 57.6. apakšpunktā minēto gadījumu;
57.8. IS nav pieļaujama funkcionalitāte, kas atļauj lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;
57.9. tiek nodrošināta IS auditācijas pierakstu veidošana un uzglabāšana vismaz sešus mēnešus pēc ieraksta izdarīšanas;
57.10. IS funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām.
58. LBTU nodrošina, lai paaugstinātas drošības IS tiktu realizētas, papildus pamata drošības sistēmas prasībām, vismaz šādas prasības:
58.1. katram lietotājam parole ir obligāti jāmaina ne vēlāk kā pēc 90 dienām, taču paroli nav atļauts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā;
58.2. lietotāja parole jāizvēlas tā, lai tā nesakristu ne ar vienu no piecām iepriekšējām lietotāja parolēm;
58.3. piecas secīgas reizes nepareizi ievadot lietotāja konta paroli, konts (izņemot administratora kontu) nekavējoties tiek bloķēts;
58.4. lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai lietotājs pašrocīgi vai ar IS atbalsta personāla palīdzību atrisinātu kļūdu;
58.5. piekļuvei pie IS administratora konta, ārpus LBTU tīkla, tiek veikta, izmantojot daudzfaktoru autentifikāciju;
58.6. tiek nodrošināta IS pierakstu veidošana un uzglabāšana vismaz 18 mēnešus pēc ieraksta izdarīšanas;

XVII. Ārpakalpojumu drošības pārvaldība

59. Ārpakalpojumu nodrošināšana IKT jomā LBTU tiek veikta saskaņā ar atbilstošu līgumu.
60. LBTU nodrošina, ka ārpakalpojuma līgumā iekļautās IKT drošības prasības nav zemākas, kā noteiktas LBTU spēkā esošajos normatīvajos aktos. Līgumā iekļauj:
60.1. detalizētu saņemamā ārpakalpojuma aprakstu;
60.2. precīzas prasības, kas saistītas ar ārpakalpojuma apjomu un kvalitāti;
60.3. prasības saistībā ar fizisko personu datu apstrādi atbilstoši normatīvajiem aktiem;
60.4. LBTU un ārpakalpojuma sniedzēju tiesības un pienākumus.
61. Ārpakalpojumu sniedzējiem ir jāparaksta un jāievēro konfidencialitātes vienošanās, kas ietver LBTU ierobežotas pieejamības informācijas izpaušanas aizliegumu. Šī vienošanās tiek slēgta gadījumos, ja konfidencialitātes nosacījumi nav iekļauti līguma pamattekstā.

XVIII. Incidentu pārvaldība

62. Incidentu pārvaldības uzdevums ir samazināt kaitējumu, kas rodas IKT drošības incidentu gadījumā.
63. Incidentu pārvaldībai LBTU nodrošina tehnisku un organizatorisku pasākumu kopumu, ievērojot IKT drošības reglamentējošajos dokumentos noteiktos principus un prasības.
64. Konstatējot drošības incidentu vai radušās aizdomas par to, personai par to nekavējoties jāziņo LBTU IT sistēmu drošības pārvaldniekam (pa e-pastu: itdrosiba@lbtu.lv), kurš sadarbībā ar IS pārvaldību atbildīgajām personām, veic informācijas pārbaudi un nepieciešamības gadījumos organizē incidenta novēršanas pasākumus.

XIX. Darbības nepārtrauktības drošības aspekti

65. IS darbības nepārtrauktību nodrošina saskaņā ar IS darbības atjaunošanas plānu un saistošām procedūrām.
66. Gadījumos, kad LBTU pārvaldībā esošās informācijas vai tehniskie resursi nav pieejami pilnā apjomā, vai pieeja tiem tiks traucēta, LBTU nodrošina lietotāju informēšanu, nosūtot par to informatīvu e-pastu vai izvietojot informāciju LBTU iekštīklā, vai konkrētajā IS.

XX. Noslēguma jautājumi

67. Drošības politiku aktualizē, ja tiek konstatēta atbilstoša nepieciešamība, un pārskata vismaz reizi gadā, kā arī gadījumos ja:
    67.1. izmaiņas IS var ietekmēt tās drošību;
    67.2. mainījušies vai ir atklāti jauni IKT drošības apdraudējumi;
    67.3. noticis nozīmīgs IKT drošības incidents;
    67.4. izmaiņas LBTU organizatoriskajā struktūrā skar IKT drošības pārvaldības organizāciju;
    67.5. izdarīti grozījumi spēkā esošajos normatīvajos aktos, kas regulē IKT jomu.
68. Drošības politikā minētie principi LBTU tiek realizēti, izvērtējot LBTU pieejamos finansiālos līdzekļus un cilvēku resursus.
69. Drošības politikas stājās spēkā ar tās apstiprināšanas dienu.