APSTIPRINĀTS
ar LU Padomes 13.05.2024.
lēmumu Nr. 1-48/29

LATVIJAS UNIVERSITĀTES INFORMĀCIJAS DROŠĪBAS POLITIKA

I. Vispārējie noteikumi

1. Latvijas Universitātes (turpmāk – LU) Informācijas drošības politika (turpmāk – Politika) nosaka vispārējus, skaidrus un saprotamus informācijas drošības mērķus, pamatprincipus, uzdevumus un pamatprasības LU personālam (darbiniekiem un studējošajiem), kā arī citiem LU informācijas tehnoloģiju sistēmu (turpmāk – IT sistēma) lietotājiem.

2. Politikā lietoti šādi termini:

2.1. Informācijas sistēma – datu ievadīšanas, uzglabāšanas, apstrādes un pārraidīšanas sistēma, kurā glabātajiem datiem vai informācijai ir paredzēta Sistēmas lietotāju pieeja vai kas lietotājiem sniedz informācijas pakalpojumus;

2.2. Informācijas resursi – LU rīcībā esošas (radītas vai saņemtas) ziņas, fakti vai ziņu un faktu kopums jebkurā tehniski iespējamā fiksēšanas, uzglabāšanas vai nodošanas veidā;

2.3. Tehniskie resursi – fiziskie serveri un tajos uzstādāmā serveru programmatūra, datu krātuves, gala lietotāju datori, datortīklu aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai;

2.4. Tīkla resursi – programmiskais, tehniskais, informacionālais un organizatoriskais datoru tīkla nodrošinājums, kas paredzēts lietotāju uzdevumu risināšanai;

2.5. Resursu lietotājs – persona, kurai ir tiesības piekļūt un veikt darbības noteiktā Informācijas sistēmā vai Tīkla resursā;

2.6. Resursu turētājs – LU rektors vai ar LU rektora rīkojumu norīkots darbinieks, kurš ir atbildīgs par informācijas tehnoloģiju (turpmāk – IT) drošības pārvaldību;

2.7. IT drošības pārvaldnieks – ar LU rīkojumu norīkots darbinieks vai ārpakalpojumu sniedzējs, kurš nodrošina IT drošības pārvaldības īstenošanu LU (*Informācijas tehnoloģiju drošības likuma izpratnē atbildīgā persona*);

2.8. Atbildīgā persona – persona, kuras kompetencē atrodas informācijas, Informācijas sistēmas vai Tehniskā resursa pārvaldība;

2.9. Resursu administrators – resursu turētāja vai ārpakalpojumu sniedzēja norīkota persona, kura ir atbildīga par resursu funkcionēšanu un datu korektu attēlošanu;

2.10. Zaudējums – jebkāds LU mantas samazinājums, zudums vai bojājums, ienākumu samazinājums, papildu izdevums vai citi mantiski novērtējami tiesību aizskārumi;

2.11. Drošības pārvaldība – nepieciešamo resursu un veikto/veicamo pasākumu kopums, lai nodrošinātu informācijas drošības pasākumu īstenošanu LU atbilstoši Politikā noteiktajam.

2.12. Mobilā ierīce - jebkura rokā turama vai pārnēsājama skaitļošanas ierīce, kurā darbojas mobilajai skaitļošanai optimizēta vai izstrādāta operētājsistēma, piemēram, Android, Apple iOS vai Windows Mobile. Neviena ierīce, kurā darbojas pilna darbvirsmas versijas operētājsistēma, nav iekļauta šajā definīcijā.

3. Politikas galvenais mērķis ir nodrošināt LU izmantoto informācijas sistēmu, saistīto tehnoloģisko resursu un informācijas konfidencialitāti, integritāti un pieejamību.

4. Politika definē LU vadības institūciju attieksmi, nostāju un atbalstu informācijas drošības nodrošināšanai atbilstoši LU vajadzībām, spēkā esošajiem normatīvajiem aktiem un drošības normām.

5. Politika ir noteikta atbilstoši Eiropas Savienības un Latvijas Republikas normatīvajiem aktiem, kā arī starptautiskajiem standartiem IT drošības jomā.

6. Šī Politika neattiecas uz jautājumiem, kas saistīti ar vispārēju fizisko drošību, piemēram, fizisko personu, ēku un teritoriju drošību, izņemot tādus fiziskās drošības aspektus, kas tieši ietekmē LU īpašumā vai rīcībā esošās informācijas drošību.

7. Politika aptver:

7.1. vispārējus informācijas drošības standartus LU informācijas sistēmām, ar tām saistītajai infrastruktūrai un tajās uzglabātajai un apstrādātajai informācijai;

7.2. vienotu pieeju, konfigurāciju un attieksmi, nodrošinot augstu informācijas sistēmu drošības līmeni;

7.3. vienotus pienākumus attiecībā uz informācijas drošību LU iestādēs;

7.4. LU informācijas sistēmu un informācijas, ko šīs sistēmas glabā, nosūta vai apstrādā drošību;

7.5. vispārēju LU regulējums informācijas drošības jomā;

8. LU pienākums ir nodrošināt, ka:

8.1. tās rīcībā esošo informācija apstrādā, glabā un pārvalda droši un pārbaudāmi, sniedzot tās darbiniekiem un Lietotājiem skaidri noteiktas prasības informācijas sistēmas iekārtu un resursu izmantošanā, un nodrošina Informācijas sistēmu aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem;

8.2. visi ar šo politiku saistītie normatīvie akti vai dokumenti ir saskaņoti ar šo Politiku.

9. Izstrādājot vai grozot LU iekšējos normatīvos aktus informācijas drošības un informācijas tehnoloģiju jomā, ir jāievēro Politikā noteiktās normas un principi.

II. Informācijas drošības politikas pamatprincipi

10. LU izvirza šādus stratēģiskos pamatprincipus informācijas drošības jomā:

10.1. LU darbības nepārtrauktības nodrošināšana;

10.2. Optimāla LU rīcībā esošo IT resursu izmantošana (samazinot drošības riskus);

10.3. Fizisko personu datu un ierobežotas pieejamības informācijas aizsardzība;

10.4. Ārējos normatīvajos aktos un LU līgumsaistībās noteikto informācijas aizsardzības pasākumu īstenošana un nodrošināšana;

10.5. LU reputācijas aizsardzība;

10.6. Efektīva informācijas drošības pārvaldība;

10.7. Prevencijas pasākumu informācijas un informācijas tehnoloģiju drošības jomā īstenošana un nodrošināšana;

10.8. Informācijas sistēmu, tehnisko un tehnoloģisko risinājumu pielietošana atbilstoši vispārpieņemtiem standartiem;

10.9. Sadarbība ar kompetentajām iestādēm informācijas drošības jomā.

III. Informācijas drošības politikas īstenošanas pamatuzdevumi

11. LU ir noteikts un pastāvīgi tiek pilnveidots dokumentu un pasākumu kopums, kuru īstenošana nodrošina Politikas mērķu sasniegšanu.

12. Informācijas drošības pasākumu organizēšanu un iekšējo normatīvu aktu izstrādi, papildināšanu un atjaunošanu LU veic saskaņā ar spēkā esošajiem normatīvajiem aktiem un standartiem.

13. Visi informācijas drošības nodrošināšanas un pārvaldības procesi LU ir vadāmi, tas ir, LU ir iespējas uzraudzīt procesus un komponentus, savlaicīgi atklāt informācijas drošības pārkāpumus un veikt atbilstošus pasākumus.

14. LU identificē, izvērtē un ātri reaģē uz faktiski notiekošajiem un iespējamiem informācijas drošības pārkāpumiem, kā arī veic incidentu dokumentēšanu un uzskaitīšanu.

15. LU nepārtraukti īsteno pasākumus informācijas drošības risku novērtēšanai un pārvaldīšanai, kā arī informācijas drošības līmeņa paaugstināšanai.

16. LU īsteno personāla un studējošo izglītošanu, tādējādi sekmējot katra LU resursu Lietotāja izpratni par saviem pienākumiem risku, darbības nepārtrauktības pārvaldīšanā un informācijas aizsardzības nodrošināšanā.

17. Informācijas sistēmu drošības procesu īstenošanas pasākumi LU, kas nav konkretizēti Politikā un attiecas uz visiem LU darbiniekiem, tiek noteikti un apstiprināti ar LU rektora rīkojumu.

IV. LU informācijas drošības organizācija

18. LU informācijas drošības politikas īstenošanas pārraudzību un resursu informācijas un informācijas tehnoloģiju drošības pārvaldības pilnvērtīgai funkcionēšanai piešķiršanu nodrošina LU rektors vai rektora pilnvarota persona.

19. IT drošības pārvaldību un šīs Politikas īstenošanu nodrošina IT drošības pārvaldnieks, kura pienākumi ir noteikti viņa amata aprakstā.

20. Informācijas tehnoloģiju departaments nodrošina ar IT drošības pārvaldību, šo Politiku un citiem normatīvajiem aktiem saistīto IT drošības pasākumu īstenošanu LU.

21. LU informācijas drošības pārvaldību balsta uz normatīvo aktu prasībām, kas precīzi un nepārprotami definē Informācijas sistēmas Lietotāja, Informācijas sistēmas atbildīgā, Informācijas sistēmas resursa atbildīgā, Informācijas sistēmas Tehniskā resursa atbildīgā, ārpakalpojuma sniedzēja un IT drošības pārvaldnieka pienākumus un tiesības darbojoties ar LU resursiem.

22. Informācijas sistēmas Lietotāja pienākumi:

22.1. ievērot šīs Politikas un citu ārējo un LU iekšējo normatīvo aktu noteikumus, kā arī rūpēties par informācijas resursu konfidencialitātes, pieejamības un integritātes saglabāšanu LU;

22.2. izmantot LU piešķirtos identifikācijas un komunikācijas rīkus, jo īpaši studiju procesā, pildot darba pienākumus un LU iekšējā saziņas procesā.

23. Informācijas sistēmas Lietotājs ir atbildīgs par visām darbībām, kas veiktas ar viņam piešķirto lietotājvārdu. Informācijas resursa Lietotāja pienākums ir informēt savu tiešo vadītāju vai kontaktpersonu (ja Informācijas resursa Lietotājs nav LU darbinieks) un Informācijas tehnoloģiju drošības pārvaldnieku par visiem informācijas tehnoloģiju drošības incidentiem, aizdomīgiem notikumiem vai Informācijas drošības politikas pārkāpumiem.

24. LU Darbinieki, kuru darba pienākums ir nodrošināt Informācijas sistēmu vai Tehnisko resursu darbību, ir atbildīgi par regulāru uzraudzību un preventīvu pasākumu veikšanu, lai nodrošinātu ilgtspējīgu, Politikas un normatīvo aktu prasībām atbilstošu Informācijas sistēmu darbību.

V. Politikas attiecināmības jomas un pamatprasības

25. Datu aizsardzības pamatprasības

25.1. LU atbilstoši Eiropas Savienības un Latvijas Republikas normatīvajiem aktiem nosaka datu, tajā skaitā fizisko personu datu un citas ierobežotas pieejamības informācijas apstrādes, glabāšanas un izsniegšanas kārtību.

25.2. LU klasificē un reglamentē piekļuves tiesību ierobežotas pieejamības informācijai piešķiršanas nepieciešamību un kārtību.

25.3. LU ievieš piekļuves kontroles pasākumus, tostarp lietotāja kontu pārvaldību, lai novērstu neatļautu piekļuvi ierobežotas pieejamības informācijai.

25.4. Lai aizsargātu ierobežotas pieejamības informācijas datus uzglabāšanas, pārsūtīšanas un dublēšanas procesu laikā, izmanto šifrēšanas mehānismus.

25.5. IT sistēmās ievieš datu aizsardzības kontroles, piemēram, ugunsmūri, ielaušanās atklāšanas sistēmas un pretvīrusu programmatūra, lai aizsargātu datus no nesankcionētas piekļuves vai ļaunprātīgām darbībām.

25.6. LU izveido incidentu reaģēšanas procedūras un plānu, lai ātri un efektīvi novērstu datu un privātuma pārkāpumus, informācijas un IT drošības incidentus. Lai nodrošinātu incidentu izmeklēšanu un ierobežošanu incidentus reģistrē un dokumentē.

26. Cilvēkresursu pārvaldības drošības pamatprasības

26.1. LU nodrošina piekļuvi informācijas sistēmām, tīkliem un fiziskām iekārtām darba vajadzībām, tas ir piešķir pieeju tikai tai informācijai un funkcijām, kas ir nepieciešamas konkrētā darbinieka vai Resursa lietotāja pienākumu izpildei.

26.2. Resursu lietotājiem, jo īpaši jaunajiem resursu lietotājiem nodrošina informāciju un apmācības par informācijas drošības jautājumiem LU.

26.3. Informē darbiniekus un studējošos par darbu ar ierobežotas pieejamības informāciju LU.

26.4. Īsteno piekļuves tiesību LU informācijas sistēmām un informācijai anulēšanas procedūras, pārtraucot darba tiesiskās attiecības vai citas tiesiskas attiecības ar LU. Nodrošina LU materiālo vērtību un informācijas, jo īpaši ierobežotas pieejamības informācijas nodošanu darba vadītājam vai drošu tās dzēšanu.

26.5. Darbinieku piekļuves anulēšanas procedūras ietver piekļuves LU informācijas sistēmām atcelšanu, LU ierīču vai iekārtu atgūšanu un fiziskās piekļuves (identifikācijas) datu atgriešanu.

27. Aktīvu pārvaldības pamatprasības

27.1. LU uztur precīzu un atjauninātu visu to aktīvu uzskaiti, ieskaitot aparatūru (ierīces, iekārtas), programmatūru, datus, aprīkojumu un intelektuālo īpašumu, kas pieder LU vai ko tā kontrolē.

27.2. Klasificē aktīvus, pamatojoties uz to kritiskumu, jutīgumu (sensitivitāti), vērtību un normatīvo aktu prasībām.

27.3. Nosaka aktīvu piešķiršanas un atgūšanas kārtību Resursu lietotājiem.

27.4. Izvirza un piemēro tādas iepirkumu prasības, lai nodrošinātu tādu aktīvu iegādi, kas atbilst konkrēti noteiktām drošības prasībām un standartiem.

27.5. Normatīvajos aktos noteiktā kārtībā novērtē pārdevējus un piegādātājus.

27.6. Visiem jauniegūtajiem aktīviem veic pieņemšanas pārbaudi un verifikāciju, lai nodrošinātu, ka tie atbilst konkrēti noteiktām prasībām un tiem nav nekādu drošības ievainojamību vai ļaunprātīgu programmatūru.

27.7. LU īsteno atbilstošas procedūras, lai nodotu vai atsavinātu aktīvus, tostarp datu sanitāriju (attīrīšanu, dzēšanu), aparatūras ekspluatācijas pārtraukšanu un ierobežotas pieejamības informācijas dzēšanu pirms atbrīvošanās no aktīviem vai pirms to atsavināšanas.

27.8. Veic aktīvu regulāru uzturēšanu un atjaunināšanu, lai nodrošinātu to drošu un efektīvu darbību.

27.9. Regulāri veic informācijas sistēmu ievainojamību monitoringu, novērtēšanu un programmatūras atjaunināšanu, lai novērstu un mazinātu drošības riskus.

27.10. LU īsteno atbilstošus drošības kontrolpasākumus, piemēram, piekļuves kontroli, šifrēšanu, fiziskās drošības pasākumus un uzraudzības sistēmas, lai aizsargātu aktīvus no nesankcionētas piekļuves, nozaudēšanas vai zādzības.

28. Informācijas pārvaldības pamatprasības

28.1. LU informāciju klasificē normatīvajos aktos noteiktā kārtībā, ņemot vērā informācijas raksturu (svarīgumu), saturu un ietekmi uz LU darbību.

28.2. Nosaka LU informācijas izmantošanas, uzglabāšanas un nodošanas trešajām personām kārtību, ņemot vērā normatīvo aktu prasības.

28.3. Piekļuvi LU informācijas sistēmām un datiem nodrošina, pamatojoties uz vismazāko nepieciešamo privilēģiju principu, nodrošinot lietotājiem piekļuvi tikai tai informācijai, kas nepieciešama viņu darba pienākumu veikšanai.

28.4. Nodrošina fizisko personu datu aizsardzību un personas privātuma aizsardzību.

28.5. Tiek īstenotas procedūras lietotāju kontu izveidei, izmaiņām un anulēšanai, tostarp piekļuves tiesību noņemšanai darbinieka darba attiecību izbeigšanas gadījumā.

28.6. Ievieš stingras paroles prasības un drošu paroļu pārvaldības praksi, lai aizsargātu lietotāju kontus un novērstu nesankcionētu piekļuvi.

28.7. LU nosaka datu saglabāšanas kārtību un procedūras, tajā skaitā drošu un savlaicīgu informācijas iznīcināšanu.

28.8. Ievieš procedūras (vai piesaista ārpakalpojumu) fizisko un elektronisko datu nesēju drošai iznīcināšanai, lai novērstu nesankcionētu piekļuvi vai atkopšanu.

29. Piekļuves kontroles pamatprasības

29.1. Lietotāju piekļuvi LU informācijas sistēmām nodrošina, ievērojot 26.1. punktā noteiktās prasības.

29.2. Izveido lietotāju reģistrācijas procedūras, lai pārbaudītu lietotāju identitāti, lomas un pienākumus.

29.3. Nodrošina procedūras, lai resursu lietotāji varētu pieprasīt piekļuvi konkrētām sistēmām vai resursiem ar atbilstošiem apstiprinājumiem un dokumentāciju (saskaņā ar 26.1. punktā noteikto piekļuves principu), kā arī nodrošina procedūras lietotāju kontu izveidei, maiņai un anulēšanai, tostarp piekļuves tiesību noņemšanai darbinieka darba attiecību izbeigšanas vai lomu maiņas gadījumā.

29.4. Nodrošina privileģēto kontu, piemēram, administratora kontu stingru kontroli. Tos kontrolē tikai pilnvarots personāls un tie tiek rūpīgi uzraudzīti.

29.5. Nosaka stingras prasības parolēm, ieskaitot minimālo garumu, sarežģītību un regulāru paroles maiņu.

29.6. Ievieš daudzfaktoru autentifikāciju, lai piekļūtu kritiskām informācijas sistēmām, ierobežotas pieejamības datiem vai ārējiem tīkliem.

29.7. Īsteno lomās balstītu piekļuves kontroli, lai piešķirtu piekļuves tiesības, pamatojoties uz darba pienākumiem.

29.8. Nodrošina piekļuves uzraudzību un auditēšanu. Informācijas sistēmas un tīklus konfigurē tā, lai reģistrētu piekļuves darbības un izveidotu audita žurnālus uzraudzības un incidentu reaģēšanas nolūkiem.

29.9. Veic regulāru piekļuves tiesību pārskatīšanu, lai nodrošinātu, ka lietotāju piekļuves tiesības ir atbilstošas, nepieciešamas un atbilst normatīvajiem aktiem.

30. Paroļu pamatprasības

30.1. LU informācijas sistēmu piekļuves parolēm nedrīkst noteikt zemākas prasības, kā to paredz normatīvie akti.

30.2. Resursu lietotājs ievēro šādus paroles aizsardzības pasākumus:

30.2.1. Nedrīkst izmantot bieži lietotus vārdus, paredzamus modeļus vai personisku informāciju.

30.2.2. Parolēm jābūt unikālām, un tās nedrīkst atkārtoti izmantot dažādos kontos.

30.2.3. Ieteicamais paroles garums: vismaz 14 rakstzīmes.

30.2.4. Lietotāji nedrīkst izmantot nekādas ar darbu saistītas paroles saviem personīgajiem kontiem.

30.2.5. Jebkurai personai, kurai ir aizdomas, ka tās parole varētu būt uzlauzta, ir jāziņo par incidentu un jāmaina visas attiecīgās paroles.

30.2.6. Paroles jāglabā droši, izmantojot spēcīgus šifrēšanas algoritmus, lai novērstu nesankcionētu piekļuvi vai pakļaušanu riskam.

30.2.7. Neizmantot lietojumprogrammu (piemēram, tīmekļa pārlūkprogrammu) funkciju "Atcerēties paroli".

30.2.8. Ieteicams izmantot paroļu pārvaldniekus, lai droši uzglabātu un pārvaldītu visas ar darbu saistītās paroles.

30.2.9. Paroles nedrīkst izpaust, nodot lietošanā nevienam, ieskaitot kolēģus, draugus vai ģimenes locekļus.

30.3. Informācijas sistēmas konfigurē tā, lai konta izveides un pārveidošanas laikā tiktu izpildītas prasības par paroles sarežģītību.

30.4. Izveido procedūras drošiem paroles atiestatīšanas procesiem, tostarp identitātes pārbaudei un autentifikācijai.

31. "Tīra galda" un ekrāna pamatprasības

31.1. Visu ierobežotas pieejamības informāciju fiziskā vai digitālā formātā uzglabā droši, jo īpaši laikā, kad to neizmanto.

31.2. Drukātos dokumentus, kas satur ierobežotas pieejamības informāciju uzglabā aizslēgtos skapjos vai atvilktnēs.

31.3. Dokumentus, kas normatīvajos aktos noteiktā kārtībā ir paredzēti iznīcināšanai (vai dokumentu kopijas) iznīcina drošā veidā, izmantojot dokumentu smalcinātājus vai citas drošas iznīcināšanas metodes.

31.4. Dokumentus, kas vairs nav vajadzīgi, nedrīkst atstāt bez uzraudzības uz rakstāmgaldiem.

31.5. Personīgās mantas ir jāglabā noteiktās vietās, piemēram, skapīšos vai atvilktnēs;

31.6. Lai novērstu nesankcionētu piekļuvi datoram, resursu lietotājs datora ekrānu bloķē vai iestata tā, lai tas automātiski bloķētos dīkstāves periodā. Lai aizsargātu informāciju, resursu lietotājs izmanto ekrāna bloķēšanas paroles vai citas autentifikācijas metodes.

31.7. Datora ekrānu darbstacijā novieto tā, lai līdz minimumam samazinātu ierobežotas pieejamības informācijas redzamību neautorizētām personām.

32. Darbstaciju drošības prasības

32.1. Darbstacijas konfigurē, izmantojot drošu pamatkonfigurāciju, kas ietver standartizētus drošības iestatījumus un ieteicamās programmatūras konfigurācijas.

32.2. Darba stacijas regulāri atjaunina ar jaunākajiem drošības ielāpiem un atjauninājumiem, ko nodrošina operētājsistēmas piegādātājs.

32.3. Lai nodrošinātu savlaicīgu un konsekventu drošības ielāpu izvietošanu, izmanto automatizētus ielāpu pārvaldības rīkus.

32.4. Visās darbstacijās jābūt instalētai un aktīvai atjauninātai ļaunatūras novēršanas programmatūrai.

32.5. Ļaunatūras novēršanas programmatūru konfigurē tā, lai tā veiktu regulārus skenējumus un saņemtu biežus parakstu atjauninājumus.

32.6. Darbstacijām nodrošina autentifikācijas mehānismus, kas nodrošina tikai autorizētu lietotāju piekļūšanu darbstacijai.

32.7. Darbstacijās, ko izmanto, lai apstrādātu ierobežotas pieejamības informāciju, izmanto šifrēšanas mehānismus, piemēram, pilna diska šifrēšana vai failu līmeņa šifrēšana, lai aizsargātu datus no neatļautas piekļuves zādzības vai nozaudēšanas gadījumā.

32.8. Darba stacijas datus regulāri dublē, izmantojot apstiprinātus dublēšanas risinājumus. Dublējumus uzglabā drošā vietā atsevišķi no darbstacijas, lai pasargātu no datu zudumiem.

32.9. Darbstacijas ir fiziski nodrošinātas vietās, kas pieejamas tikai LU personālam.

32.10. Mobilās darbstacijas nedrīkst atstāt bez uzraudzības publiskās vietās vai transportlīdzekļos.

33. Mobilo ierīču drošības pamatprasības

33.1. Mobilās ierīces konfigurē, izmantojot drošu pamatkonfigurāciju, kas ietver standartizētus drošības iestatījumus un ieteicamās programmatūras konfigurācijas.

33.2. Mobilās ierīces regulāri atjaunina ar jaunākajiem operētājsistēmas un lietojumprogrammu drošības ielāpiem un atjauninājumiem, ko nodrošina piegādātāji.

33.3. Lietotājiem, izmantojot mobilās ierīces, ir jāievēro LU Pieņemamās lietošanas noteikumi.

33.4. Resursu lietotāji mobilās ierīces pievieno mobilo datu pieslēgumam, LU Wi-Fi tīkliem vai izmanto virtuālos privātos tīklus (turpmāk – VPN).

33.5. Resursu lietotāji veic atbilstošos pasākumus, lai aizsargātu mobilās ierīces fiziski, piemēram, izmantojot ekrāna slēgšanu, piekļuves kodus vai biometriskās autentifikācijas mehānismus.

33.6. Mobilās ierīces nedrīkst atstāt bez uzraudzības citām personām brīvi pieejamās vietās.

34. Attālinātā piekļuve un elektronisko sakaru pamatprasības

34.1. Attālinātu piekļuvi LU resursiem piešķir, saskaņā ar 26.1. punktā noteikto principu.

34.2. Resursu lietotāji ievēro LU autentifikācijas procedūras, pirms viņi attālināti piekļūst LU informācijas sistēmām.

34.3. Resursu lietotāji izmanto apstiprinātas attālinātās piekļuves metodes, piemēram, VPN vai drošus attālinātās darbvirsmas protokolus, lai izveidotu šifrētus savienojumus starp attālajām ierīcēm un LU tīkliem.

34.4. Noklusējuma vai vājas attālinātās piekļuves konfigurācijas ir aizliegtas.

34.5. Resursu lietotāji ir atbildīgi par savu attālinātam pieslēgumam izmantoto ierīču drošības uzturēšanu, ieskaitot jaunāko operētājsistēmu, drošības ielāpu un pretvīrusu programmatūras nodrošināšanu.

34.6. Resursu lietotāji nedrīkst izmantot publiskos vai nedrošos tīklus, lai izveidotu attālus savienojumus.

34.7. Lietotājiem jāievēro attiecīgās datu aizsardzības un drošības politikas, attālināti piekļūstot un apstrādājot LU datus.

34.8. Ierobežotas pieejamības informāciju sūta un glabā šifrētā veidā.

34.9. Resursu lietotāji ir atslēdzas vai atvienojas no attālinātās sesijas pēc tam, kad ir paveikuši savus uzdevumus vai atstāj savas ierīces bez uzraudzības.

34.10. Resursu lietotāji ievēro drošas videokonferences paraugpraksi, tostarp izmanto paroles vai piekļuves kodus, lai novērstu nesankcionētu piekļuvi.

34.11. Sapulces saišu vai piekļuves akreditācijas datu koplietošanu veic droši un tikai ar autorizētiem dalībniekiem.

35. Personīgo ierīču izmantošanas pamatprasības

35.1. Personīgās ierīces atbilst minimālajām drošības prasībām, piemēram, piekļuves kodu vai biometrijas autentifikācijas iespējošanai, atjaunināto operētājsistēmu un lietojumprogrammu uzturēšanai un attālinātas dzēšanas iespējām.

35.2. Piekļūstot LU resursiem vai pārraidot ierobežotas pieejamības informāciju, ierīces veido savienojumu ar drošiem Wi-Fi tīkliem vai izmanto VPN.

35.3. Ierīcēs jābūt instalētai un aktīvai atjauninātai ļaunatūras novēršanas programmatūrai.

35.4. Ļaunatūras novēršanas programmatūru konfigurē tā, lai tā veiktu regulārus skenējumus un saņemtu biežus parakstu atjauninājumus.

35.5. Ierīcēm, ko izmanto ierobežotas pieejamības informācijas apstrādei vai glabāšanai, izmanto šifrēšanas mehānismus, piemēram, pilna diska (ierīces) šifrēšana vai failu līmeņa šifrēšana, lai aizsargātu datus no neatļautas piekļuves nozaudēšanas vai zādzības gadījumā.

35.6. Resursu lietotāji ievēro LU Pieņemamās lietošanas noteikumus, ja viņi izmanto savas personiskās ierīces ar LU saistītām darbībām vai darba pienākumu veikšanai.

35.7. Resursu lietotāji nodrošina, lai viņu darbība nekaitētu LU resursu drošībai vai integritātei un nepārkāptu piemērojamos normatīvos aktus.

35.8. Resursu lietotāji veic atbilstošus pasākumus, lai savā ierīcē atdalītu savus un LU datus, tādējādi novēršot nesankcionētu piekļuvi vai izpaušanu.

35.9. Resursu lietotāji ir atbildīgi par viņu personīgo un LU datu regulāru dublēšanu, lai novērstu datu zudumu ierīces kļūmes vai citu incidentu gadījumā.

36. Ārējo datu nesēju pamatprasības

36.1. Ir aizliegta personīgo ārējo datu nesēju ierīču izmantošana LU informācijas glabāšanai vai pārsūtīšanai.

36.2. Ir atļauts lietot tikai Eiropas Savienības tirgum paredzētas ārējās datu nesēju ierīces.

36.3. Ārējiem datu nesējiem jābūt aizsargātiem ar paroli, lai novērstu nesankcionētu piekļuvi.

36.4. Pirms ārējo datu nesēju izmantošanas LU sistēmās, noņemamie datu nesēji ir jāpārbauda, vai tajos nav ļaunprātīgas programmatūras, izmantojot atjauninātu pretvīrusu programmatūru.

36.5. Ja tiek atklāta ļaunprātīga programmatūra, ārējo datu nesēju nedrīkst savienot ar LU sistēmām, un par to ir jāziņo IT servisam.

36.6. Ierobežotas pieejamības informācija ārējo datu nesēju ierīcēs uzglabājama vienīgi objektīvi pamatotos izņēmuma gadījumos, piemēram, datu nodošana.

36.7. Ārējos datu nesējus, kad tie netiek lietoti uzglabā droši, vēlams aizslēgtos skapjos vai atvilktnēs.

36.8. Ārējās datu nesēju ierīces drīkst izmantot tikai datu pārsūtīšanai starp uzticamām sistēmām un pilnvarotām personām.

36.9. Datu pārsūtīšanas laikā izmanto datu šifrēšanu.

36.10. Datus no ārējās datu nesēja ierīces pirms iznīcināšanas vai atkārtotas izmantošanas pienācīgi izdzēš, lai nodrošinātu datu neatgriezenisku noņemšanu.

37. Šifrēšanas pamatprasības

37.1. Datu, kas ir uzglabāšanas procesā, šifrēšana:

37.1.1. Ierobežotas pieejamības informācijai, ko glabā LU vai tās kontrolētās ierīcēs, ieskaitot serverus, klēpjdatorus un mobilās ierīces, jābūt šifrētiem, izmantojot apstiprinātas šifrēšanas metodes.

37.1.2. Šifrēšanu lieto visai ierīcei vai konkrētam datu apjomam, kas satur ierobežotas pieejamības informāciju.

37.2. Nodošanas procesā esošu datu šifrēšana:

37.2.1. Ierobežotas pieejamības informāciju, ko nodod iekšējos vai ārējos tīklos, aizsargā, izmantojot šifrēšanas tehnoloģijas/protokolus.

37.2.2. Šifrēšanu izmanto e-pasta saziņai, failu pārsūtīšanai, attālās piekļuves sesijām un citām tīkla pārraidēm, kas saistītas ar ierobežotas pieejamības informāciju.

37.3. Dati, kas ir apstrādes vai lietošanas procesā:

37.3.1. Nepieciešama datu šifrēšana ierobežotas pieejamības informācijai, ko apstrādā vai kam piekļūst lietojumprogrammas, datu bāzes vai citas programmatūras sistēmas.

37.3.2. Izmanto šifrēšanas metodes, piemēram, lietojumprogrammas līmeņa šifrēšanu vai datu bāzes šifrēšanu, pamatojoties uz datu jutīgumu un saistītajiem riskiem.

37.4. Šifrēšanas atslēgu izplatīšanai un apmaiņai izmanto drošas metodes, piemēram, atslēgu apmaiņas protokolus vai drošas saziņas kanālus.

37.5. Izveido procesus, lai atceltu un aizstātu šifrēšanas atslēgas.

37.6. Veic regulāru atslēgu rotāciju (maiņu), lai samazinātu risku, kas saistīts ar atslēgu ilgtermiņa lietošanu.

38. Lietojumprogrammu drošības pamatprasības

38.1. Lietojumprogrammas drošības prasības identificē un dokumentē lietojumprogrammas izstrādes vai ieviešanas plānošanas posmā.

38.2. Drošības prasības aptver tādas jomas kā autentifikācija, piekļuves kontrole, ievades validācija, šifrēšana, kļūdu apstrāde un reģistrēšana.

38.3. Izstrādātāji ievēro drošu kodēšanas praksi, ieskaitot ievades validāciju, izvades kodēšanu, drošu sesiju pārvaldību un drošu konfigurāciju.

38.4. Tiek ievērotas drošas kodēšanas vadlīnijas, lai risinātu vispārējas lietojumprogrammu drošības problēmas.

38.5. Lietojumiem veic regulārus ievainojamības novērtējumus, tostarp automatizētu skenēšanu un manuālas ielaušanās pārbaudes.

38.6. Atklātās ievainojamības prioritizē, pamatojoties uz ievainojamību bīstamību, un tās novērš savlaicīgi.

38.7. Kodu pārskatīšanu veic, lai noteiktu kodēšanas kļūdas, drošības ievainojamības un lai ievērotu drošas kodēšanas praksi.

38.8. Lai identificētu vājās vietas un novērtētu drošības kontroļu efektivitāti, lietojumprogrammām veic drošības pārbaudes, tostarp ielaušanās testus.

38.9. Testus veic gan izstrādes posmā, gan pēc lietojumprogrammu atjauninājumiem vai būtiskām izmaiņām.

38.10. Lietojumprogrammas uzstāda, izmantojot drošus konfigurācijas iestatījumus un vadlīnijas, ko nodrošina programmu piegādātāji vai izstrādātāji.

38.11. Noklusējuma paroles, nevajadzīgas funkcijas un nedrošus protokolus atspējo vai noņem.

38.12. Lietojumprogrammas atjaunina ar jaunākajiem drošības ielāpiem un atjauninājumiem, ko nodrošina piegādātāji.

38.13. Integrējot lietojumprogrammas ar citām sistēmām vai trešo personu komponentiem, jāņem vērā drošības apsvērumi, lai nodrošinātu datu integritāti un konfidencialitāti.

39. Sociālo mediju pamatprasības

39.1. Tikai LU izraudzītas pilnvarotas personas var veidot un pārvaldīt LU oficiālos sociālo mediju kontus.

39.2. Oficiālos sociālo plašsaziņas līdzekļu kontus pārvalda LU noteiktā kārtībā.

39.3. Izmantojot sociālo plašsaziņas līdzekļu platformas ievēro privātuma, konfidencialitātes un intelektuālā īpašuma tiesības.

40. Datu rezerves kopiju veidošanas pamatprasības

40.1. LU pamatojoties uz datu klasifikāciju, izmanto dažādas dublēšanas stratēģijas, saglabāšanas periodus un glabāšanas metodes.

40.2. Dublēšanas grafikus nosaka, pamatojoties uz LU atjaunošanas punktu mērķiem (RPO) un datu kritiskumu.

40.3. Veic regulāru datu dublēšana, lai fiksētu izmaiņas un atjauninājumus kopš pēdējās dublēšanas.

40.4. Var izmantot pilno, inkrementālo un diferenciālo dublēšanas metožu kombināciju, pamatojoties uz datu kritiskumu, izmaiņu biežumu un atjaunošanas laika mērķiem (RTO).

40.5. Dublētie dati, jo īpaši ierobežotas pieejamības informācija, jāšifrē tranzīta un uzglabāšanas laikā, lai nodrošinātu tās konfidencialitāti un integritāti.

40.6. Dublējumkopijas glabā neklātienē, lai aizsargātu pret lokalizētām katastrofām, piemēram, ugunsgrēku, plūdiem vai zādzībām.

40.7. Neklātienes vietu krātuvēm jābūt drošām un aprīkotām ar atbilstošu vides kontroli, lai aizsargātu dublējumkopijas.

40.8. Dublējuma datu saglabāšanas periodus nosaka, pamatojoties uz tiesiskām, regulatīvām un darbības prasībām.

40.9. Dublējuma datu glabāšanas laiku nosaka, ievērojot sistēmu individuālās prasības, un ievērojot iespēju atgūties no datu zuduma vai sistēmas kļūmēm pieņemamos termiņos.

40.10. Datu dublējumus, kas vairs nav nepieciešami, iznīcina drošā veidā, izmantojot apstiprinātas datu iznīcināšanas metodes, piemēram, drošu dzēšanu vai fizisku iznīcināšanu.

40.11. Par dublēšanu atbildīgā persona nodrošina dublēšanas procesu pārraudzību, ieskaitot plānošanu un testēšanu.

40.12. Par dublēšanu atbildīgā persona nodrošina, ka tiek ievērotas dublēšanas procedūras, dublēšana tiek veiksmīgi pabeigta un dublēšanas datu nesēji tiek pareizi pārvaldīti.

40.13. Datu īpašnieki sadarbībā ar par dublēšanu atbildīgo personu identificē datu kritiskuma un dublēšanas prasības un nodrošina nepieciešamo atbalstu dublēšanas un atkopšanas darbībām.

41. Ļaunatūras aizsardzības pamatprasības

41.1. Visām LU piederošām vai kontrolētām ierīcēm, ieskaitot serverus, darbstacijas un mobilās ierīces, jābūt instalētai un konfigurētai atjauninātai pretvīrusu/ļaunatūras novēršanas programmatūrai.

41.2. Pretvīrusu/ļaunprogrammatūras novēršanas programmatūrai jābūt pieejamai reāllaika skenēšanai, automātiskiem atjauninājumiem un zināmas un nezināmas ļaunprogrammatūras atklāšanai/noņemšanai.

41.3. Visām LU izmantotajām lietojumprogrammām, operētājsistēmām un programmatūrai jābūt atjauninātām ar jaunākajiem drošības ielāpiem un kļūdu labojumiem.

41.4. LU ievieš drošības ielāpu pārvaldības procedūras, lai nodrošinātu savlaicīgu atjauninājumu uzstādīšanu un mazinātu ievainojamību, ko rada ļaunatūra.

41.5. Informācijas sistēmām jābūt nostiprinātām, tajā skaitā, atspējojot nevajadzīgus pakalpojumus un funkcijas, nodrošinot ugunsmūrus un ieviešot piekļuves kontroles.

41.6. Sistēmas noklusējuma konfigurācijas tiek mainītas, lai samazinātu iespējamo ievainojamību, ko var radīt ļaunatūra.

41.7. Ievieš e-pasta filtrēšanas mehānismus lai skenētu ienākošos un izejošos e-pasta ziņojumus par ļaunatūras pielikumiem un ļaunprātīgām saitēm.

41.8. Īsteno tīmekļa drošības pasākumus, piemēram, tīmekļa satura filtrēšanu un piekļuves bloķēšanu ļaunprātīgām vietnēm, lai aizsargātu lietotājus no ļaunatūras lejupielādēšanas vai piekļuves ļaunatūrai.

41.9. Ievieš tīkla segmentāciju un piekļuves kontroles, lai novērstu ļaunprātīgu programmatūru izplatību LU tīklā.

41.10. Lai atklātu un bloķētu ļaunatūras datplūsmu, izvieto ielaušanās atklāšanas un novēršanas sistēmas (IDS/IPS).

42. Tīkla aizsardzības pamatprasības

42.1. LU tīkla infrastruktūru segmentē loģiski nošķirtās zonās, lai samazinātu iespējamo drošības pārkāpumu ietekmi un ierobežotu uzbrukumu izplatību.

42.2. Uztur visaptverošas un atjauninātas tīkla shēmas, lai sniegtu pārskatu par LU tīkla topoloģiju un palīdzētu tīklu aizsardzības plānošanā un pārvaldībā.

42.3. Ievieš piekļuves kontroles mehānismus, piemēram, ugunsmūri, ielaušanās novēršanas sistēmas (IPS) un virtuālos tīklus (VLAN), lai regulētu un kontrolētu informācijas plūsmu starp dažādiem tīkla segmentiem.

42.4. Tīkla iekārtām, ieskaitot maršrutētājus, slēdžus, ugunsmūrus un bezvadu piekļuves punktus, jābūt droši konfigurētām saskaņā ražotāja norādījumiem.

42.5. Noklusējuma vai vājās konfigurācijas ir jāmaina, nevajadzīgie pakalpojumi ir jāatspējo un jāaktivizē drošie protokoli.

42.6. Tīkla iekārtas regulāri jāatjaunina, izmantojot jaunākos piegādātāju piedāvātos ielāpus un programmaparatūras atjauninājumus, lai novērstu zināmās ievainojamības.

42.7. Nodrošina drošības ielāpu pārvaldības procesu.

42.8. Piekļuve tīkla ierīcēm ir atļauta tikai pilnvarotam personālam, pamatojoties uz vismazāko nepieciešamo privilēģiju principu.

42.9. Lai atklātu iespējamos drošības incidentus un reaģētu uz tiem, ir jāveic nepārtraukta tīkla informācijas plūsmas uzraudzība, tostarp ieejas un izejas punktu uzraudzība.

42.10. Lai identificētu un mazinātu ļaunprātīgas darbības, izmanto tīkla uzraudzības instrumentus, piemēram, ielaušanās atklāšanas sistēmas (IDS) un ielaušanās novēršanas sistēmas (IPS).

42.11. Bezvadu tīkliem izmanto šifrēšanas protokolus, piemēram, WPA2 vai WPA3, lai aizsargātu bezvadu sakarus. Izvairās no noklusējuma vai vājiem šifrēšanas iestatījumiem, piemēram, WEP.

42.12. Bezvadu piekļuves punktus konfigurē, lai ieviestu spēcīgus autentifikācijas un autorizācijas mehānismus.

42.13. Viesu bezvadu tīklus izolē no iekšējā tīkla resursiem un tiem piemēro piekļuves ierobežojumus.

43. Reģistrācijas un uzraudzības pamatprasības

43.1. LU informācijas sistēmām un tīkla ierīcēm rada žurnālus, kuros reģistrē attiecīgos drošības notikumus, tostarp, bet ne tikai, autentifikācijas notikumus, piekļuves kontroles notikumus, sistēmas konfigurācijas izmaiņas un drošības incidentus.

43.2. Žurnālus aizsargā pret nesankcionētu piekļuvi, grozīšanu vai dzēšanu, lai nodrošinātu to integritāti un uzticamību kā pierādījumu drošības izmeklēšanā.

43.3. Žurnālfailus aizsargā, ieviešot šifrēšanas, piekļuves kontroles un dublēšanas procedūras.

43.4. Žurnālus regulāri uzrauga un analizē, izmantojot atbilstošus rīkus un metodes, lai noteiktu drošības notikumus, anomālijas vai kompromitēšanas indikatorus.

43.5. LU ievieš žurnālu uzraudzības rīkus un tehnoloģijas, piemēram, drošības informācijas un notikumu pārvaldības sistēmas, lai automatizētu žurnālu vākšanu, analīzi un brīdināšanu.

44. Sistēmu izmaiņu un konfigurācijas pamatprasības

44.1. Izmaiņu pieprasījumus izvērtē, pamatojoties uz to iespējamo ietekmi, riskiem un ieguvumiem. Lai novērtētu ierosinātās izmaiņas, ievēro pienācīgas testēšanas un novērtēšanas procedūras.

44.2. LU saglabā visu izmaiņu dokumentāciju, tostarp izmaiņu aprakstu, īstenošanas plānu un atrites procedūras.

44.3. Pamatkonfigurācijām jābūt dokumentētām, kontrolētām un regulāri pārbaudītām attiecībā uz precizitāti un atbilstību.

44.4. Konfigurācijas izmaiņas apstiprina, pārbauda, dokumentē un ievieš kontrolētā veidā.

44.5. Veic regulāru informācijas sistēmu konfigurāciju uzraudzību, lai identificētu un labotu visas neautorizētās vai nekonsekventās konfigurācijas.

44.6. Izmaiņām, īpaši tām, kas var ietekmēt sistēmas funkcionalitāti vai drošību, pirms to ieviešanas veic testēšanu kontrolētā vidē.

44.7. Testēšanā iekļauj funkcionalitātes testēšanu, ievainojamības pārbaudi un drošības testēšanu.

44.8. Attiecībā uz katru izmaiņu nosaka un dokumentē atrites procedūras, lai jautājumu vai neparedzētu seku gadījumā atgrieztos iepriekšējā zināmā labā stāvoklī.

44.9. LU ievieš mehānismus, lai uzraudzītu un reģistrētu sistēmas izmaiņas, konfigurācijas un ar tām saistīto darbību auditus.

45. Atjaunināšanas pamatprasības

45.1. LU regulāri veic ievainojamību skenēšanu, izmantojot nozares standarta rīkus, lai identificētu LU informācijas sistēmu, lietojumprogrammu un ierīču ievainojamības un prioritizētu tās.

45.2. Skenēšana ietver gan iekšējos, gan ārējos novērtējumus, lai identificētu iespējamās nepilnības un ievainojamības.

45.3. Identificētās ievainojamības novērtē un prioritizē, pamatojoties uz to nopietnību, iespējamo ietekmi uz LU informācijas līdzekļiem un izmantošanas iespējamību.

45.4. LU uztur attiecīgo drošības adresātu sarakstu un paziņojumu abonementus, lai saņemtu informāciju par jaunākajiem drošības ielāpiem un ievainojamību.

45.5. Izvērtē drošības ielāpu atbilstību, piemērojamību un iespējamo ietekmi uz informācijas sistēmas funkcionalitāti, stabilitāti un saderību ar esošo programmatūru un konfigurāciju.

45.6. Novērtēšanas procesā ņem vērā riska līmeni, kas saistīts ar katru ievainojamību, un piegādātāja nodrošināto drošības ielāpu pieejamību.

45.7. Kritiskajiem drošības ielāpiem, kas novērš augsta riska ievainojamības piešķir augstāko prioritāti tūlītējai uzstādīšanai.

45.8. Pirms uzstādīšanas ražošanas vidē drošības ielāpus pārbauda kontrolētā un izolētā vidē.

45.9. Testēšanas procedūras ietver funkcionālo un saderības testēšanu, lai nodrošinātu, ka drošības ielāpi nerada konfliktus un netraucē normālu sistēmu darbību.

45.10. Drošības ielāpu uzstādīšana var būt pakāpeniska, lai samazinātu ietekmi uz kritiskajām sistēmām un nodrošinātu iespēju pārraudzīt un risināt neparedzētas problēmas.

45.11. LU izmantos drošības ielāpu pārvaldības rīkus un sistēmas, lai automatizētu ielāpu uzstādīšanas procesu un nodrošinātu centralizētu pārredzamību un kontroli.

45.12. Kritisku ievainojamību vai nulles dienas ekspluatācijas gadījumā ievēros ārkārtas drošības ielāpu uzstādīšanas procedūras, lai paātrinātu ielāpu uzstādīšanu.

45.13. LU regulāri pārraudzīs informācijas sistēmas, lai nodrošinātu ielāpu atbilstību un pārbaudītu, vai ielāpi ir uzstādīti, kā paredzēts.

45.14. Pēc drošības ielāpu uzstādīšanas veiks verifikāciju, lai apstiprinātu, ka drošības ielāpi ir instalēti sekmīgi, un apstiprinātu atjaunināto sistēmu nepārtrauktu funkcionalitāti un stabilitāti.

45.15. Saglabā visaptverošus datus par visām ar drošības ielāpu lietošanu saistītajām darbībām, ieskaitot drošības ielāpu novērtējumus, uzstādīšanas plānus, testēšanas rezultātus un verifikācijas ziņojumus.

45.16. Sistēmu administratori ir atbildīgi par to, lai viņu attiecīgajās informācijas sistēmās savlaicīgi tiktu uzstādīti drošības ielāpi.

46. Licencēšanas pamatprasības

46.1. LU nosaka centralizētu programmatūras iepirkuma procesu, kas ietver pārskatīšanas un apstiprināšanas mehānismu.

46.2. Pirms jaunas programmatūras iegādes atbilstošajam personālam jānovērtē programmatūras licencēšanas noteikumi, saderība un drošības prasības.

46.3. Visas programmatūras licences izvērtē, lai nodrošinātu atbilstību piemērojamiem normatīvajiem aktiem un licencēšanas noteikumiem.

46.4. LU uztur precīzu un atjauninātu visu programmatūras licenču uzskaiti, ieskaitot tādas detaļas kā licenču veidi, daudzumi, versijas un pārdevēji.

46.5. Regulāri uzrauga programmatūras licenču izmantošanu, lai nodrošinātu atbilstību licenču noteikumiem un nosacījumiem.

46.6. Sagatavo izmantošanas ziņojumus, lai identificētu jebkādas neatbilstības vai licences nepareizas izmantošanas gadījumus.

46.7. Licenču atjaunošanu uzsāk savlaicīgi, lai izvairītos no programmatūras lietošanas traucējumiem, ko rada licences, kurām beidzies derīguma termiņš.

46.8. Veic regulārus auditus, lai pārbaudītu atbilstību programmatūras licences līgumiem.

46.9. Saglabā precīzu programmatūras licenču uzskaiti, ieskaitot pirkuma apliecinājumu, licences līgumus un uzturēšanas līgumus.

46.10. Auditēšanas nolūkos saglabā visaptverošus ziņojumus par programmatūras licencēšanas statusu, lietojumu un atbilstību.

47. Mākoņdatošanas drošības pamatprasības

47.1. Pirms sadarbošanās ar mākoņpakalpojumu sniedzēju veic rūpīgu novērtējumu, lai novērtētu drošības kontroles, sertifikātus, atbilstību un darbības rezultātus.

48. Sistēmas iegūšanas pamatprasības

48.1. Pirms jebkura sistēmas iegūšanas procesa uzsākšanas veic visaptverošu vajadzību novērtējumu, lai noteiktu un dokumentētu LU īpašās prasības, tostarp funkcionālās, tehniskās un drošības prasības. Vajadzību novērtējumā iesaista attiecīgās ieinteresētās personas, piemēram, galalietotāji, IT darbinieki un iestāžu vadītāji, lai nodrošinātu visaptverošu izpratni par prasībām.

48.2. Piegādātāji, kas piedāvā informācijas sistēmas un saistītos aktīvus, ir jānovērtē, pamatojoties uz iepriekš noteiktiem kritērijiem, tostarp to drošības iespējām, sasniegumiem, atsaucēm un atbilstību attiecīgajiem standartiem un sistēmām.

48.3. Novērtēšanas procesā iekļauj rūpīgu piegādātāja drošības politikas, procedūru un kontroļu pārbaudi, kā arī viņu apņemšanos nodrošināt pastāvīgus drošības atjauninājumus un atbalstu.

48.4. Visām iegūtajām informācijas sistēmām jāatbilst LU obligātajām drošības prasībām, kas noteiktas šajā politikā, normatīvajos aktos un attiecīgajos nozares standartos.

48.5. Pirms jebkuras iegūtās sistēmas uzstādīšanas jāveic visaptverošs testēšanas un pieņemšanas process, lai pārliecinātos par tās funkcionalitāti, veiktspēju un drošību.

48.6. Pieņemšanas kritēriji jānosaka un par tiem jāvienojas ar pārdevēju pirms sistēmas galīgās pieņemšanas.

48.7. Jāveic drošības testēšana, tostarp ievainojamību novērtēšana un ielaušanās pārbaude.

48.8. Sistēmu konfigurācijām jābūt saskaņotām ar drošības norādījumiem, ko nodrošina sistēmas piegādātājs un attiecīgie standarti.

49. Līgumu un piegādātāju drošības pamatprasības

49.1. Piegādātājus novērtē, pamatojoties uz iepriekš definētiem kritērijiem, kas ietver viņu drošības iespējas, ierakstu izsekošanu, atsauces un atbilstību attiecīgajiem drošības standartiem un regulējumiem.

49.2. Novērtēšanas procesā ņem vērā tādus faktorus kā piegādātāja drošības politika, procedūras, kontroles, incidentu reaģēšanas spējas un viņu apņemšanās pastāvīgi atjaunināt drošību un sniegt atbalstu.

49.3. Piegādātājiem var tikt veikti drošības novērtējumi, lai novērtētu viņu drošības stāvokli un atbilstību LU drošības prasībām.

49.4. Drošības novērtējumi var ietvert apmeklējumus uz vietas, auditus, ielaušanās testēšanu, ievainojamības novērtējumus, drošības politikas, procedūru un kontroļu pārskatus.

49.5. Drošības novērtējumu biežums un apjoms jānosaka, pamatojoties uz piegādātāja sniegto pakalpojumu kritiskumu un jutīgumu.

49.6. LU IT departaments regulāri uzrauga piegādātāju drošības praksi un līgumsaistību ievērošanu.

49.7. Uzraudzības darbības var ietvert drošības ziņojumu pārskatīšanu, auditu veikšanu un pierādījumu pieprasīšanu par atbilstību drošības kontrolēm un standartiem.

49.8. Piegādātājiem nekavējoties jāziņo par visiem drošības starpgadījumiem vai pārkāpumiem, kas var ietekmēt LU datus, informācijas sistēmas vai pakalpojumus.

49.9. Piegādātājiem jābūt dokumentētiem darbības nepārtrauktības un katastrofu seku novēršanas plāniem, lai nodrošinātu nepārtrauktu pakalpojumu sniegšanu traucējumu gadījumā.

49.10. Līgumu izbeigšanas procesā jāiekļauj procedūras LU datu un aktīvu drošai noņemšanai vai pārsūtīšanai no piegādātāja sistēmām.

49.11. Kad piegādātāja attiecības tiek izbeigtas vai beidzas termiņš, ir jāievēro atbilstošas izslēgšanas procedūras, lai nodrošinātu visu LU piederošo datu, aktīvu vai piegādātāja īpašumā esošo intelektuālā īpašuma atgriešanu vai iznīcināšanu.

49.12. Izslēgšanas procesā iekļauj piekļuves tiesību atņemšanu, piekļuves akreditācijas datu atsaukšana un datu sanitārijas vai iznīcināšanas apstiprināšanu.

50. Novecojušās IT aparatūras un programmatūras drošības pamatprasības

50.1. LU uzskaita un novērtē novecojušo IT aparatūru un programmatūru.

50.2. Novecojušo IT aparatūru un programmatūru nosaka, pamatojoties uz tādiem kritērijiem kā vecums, neatbalstītas operētājsistēmas, neatbalstītas lietojumprogrammas, dzīves beigu (nolietojums) statuss un piegādātāju atbalsta trūkums.

50.3. Novecojušo IT aparatūru un programmatūru izolē no galvenā tīkla, lai ierobežotu to pakļaušanu ārējiem apdraudējumiem.

50.4. LU ievieš tīkla segmentāciju un ugunsmūri, lai ierobežotu piekļuvi novecojušajai IT aparatūrai un programmatūrai un nodrošinātu detalizētāku kontroli pār tīkla datu plūsmu.

50.5. Ierobežo piekļuvi novecojušajai IT aparatūrai un programmatūrai.

50.6. Novecojušajā IT aparatūrā saglabātie dati jāmigrē uz jaunākām, atbalstītām sistēmām, ievērojot atbilstošas datu migrācijas procedūras.

50.7. Lai novērstu datu noplūdi un nesankcionētu piekļuvi, izbeidzot novecojušo IT aparatūras un programmatūras ekspluatāciju, ir jāveic atbilstošas iznīcināšanas procedūras.

51. Sanitārijas, atkārtotas izmantošanas un iznīcināšanas pamatprasības

51.1. Pirms jebkādu informācijas līdzekļu atkārtotas izmantošanas vai iznīcināšanas veic datu dzēšanu.

51.2. Informācijas līdzekļus, kurus nevar izmantot atkārtoti iznīcina.

52. Mākslīgā intelekta (turpmāk – MI) risinājumu izmantošanas darba vietā pamatprasības

52.1. Darba vietā izmantotajiem MI algoritmiem un modeļiem jābūt izstrādātiem tā, lai tie būtu godīgi, pārredzami un nediskriminējoši, kā arī tādi, kas atbilst LU kā augstākās izglītības iestādes darbības principiem, jo īpaši akadēmiskā godīguma jomā.

52.2. MI risinājumiem ir jāatbilst fizisko personu datu aizsardzības normatīvajiem aktiem, nodrošinot personas datu privātumu un drošību.

52.3. Datu apstrādes darbībām, ko veic MI sistēmas, jābūt pārredzamām attiecībā uz personām, un vajadzības gadījumā jāievieš piemēroti piekrišanas mehānismi.

52.4. MI risinājumu lietotājiem jābūt skaidrai izpratnei par to, kā tiek pieņemti lēmumi, un par faktoriem, kas ietekmē šos lēmumus.

52.5. LU nosaka skaidras prasības un aprakstus MI risinājumu izstrādei, ieviešanai un uzturēšanai.

52.6. LU nodrošinās, ka personāls, kas izmanto MI risinājumus, ir pienācīgi apmācīts un informēts.

52.7. MI risinājumiem pirms to ieviešanas veic testēšanu, validēšanu un kvalitātes novērtēšanu.

53. Darbības nepārtrauktības pārvaldības pamatprasības

53.1. Izstrādā darbības nepārtrauktības plānu svarīgām darbības funkcijām un pakalpojumiem, pamatojoties uz darbības ietekmes analīzi un riska novērtējumu.

53.2. Darbības nepārtrauktības plānu regulāri pārskata un atjaunina, lai nodrošinātu tā efektivitāti un atbilstību organizācijas izmaiņām.

53.3. Veiks regulāras pārbaudes un mācības, lai apstiprinātu darbības nepārtrauktības plānu efektivitāti un personāla gatavību.

53.4. Atjaunošanas stratēģijas un plāni tiks īstenoti, lai atjaunotu kritiskās operācijas un pakalpojumus noteiktajā atjaunošanas laikā (RTO).

53.5. Pēc incidenta veic darbību pārskatīšanu, lai noteiktu gūto pieredzi un uzlabojumus turpmākajai reaģēšanai uz incidentiem un darbības atjaunošanai.

54. Drošības incidentu pārvaldības (procedūras) pamatprasības

54.1. Visiem resursu lietotājiem ir pienākums nekavējoties ziņot par visiem iespējamiem vai apstiprinātiem drošības incidentiem.

54.2. Informācija par ziņošanas kanāliem par incidentu, tostarp noteiktās incidentu reaģēšanas grupas kontaktinformācija, ir publiski pieejama.

54.3. Ir noteikts incidentu reaģēšanas plāns, kurā noteiktas reaģēšanas un seku mazināšanas darbības dažāda veida drošības incidentu gadījumā.

54.4. Incidentu reaģēšanas plānā iekļauj procedūras incidenta ierobežošanai, pierādījumu saglabāšanai, ekspertīzes veikšanai un atbilstošu sanācijas pasākumu īstenošanai.

54.5. Gadījumos, kad drošības incidentam nepieciešama turpmāka izmeklēšana, jābūt norīkotai grupai vai personai, kas būs atbildīga par rūpīgas izmeklēšanas veikšanu.

54.6. Incidentu reaģēšanas grupa izveido saziņas kanālus, lai nodrošinātu savlaicīgu un precīzu informācijas apmaiņu.

54.7. Visus drošības incidentus, tostarp to datus, ietekmes novērtējumus, atbildes pasākumus un rezultātus dokumentē incidenta ziņojumā.

54.8. Ziņojumus par incidentiem ir saglabā turpmākai uzziņai, gūtās pieredzes apkopošanai un atbilstības prasībām.

54.9. Pēc katra drošības incidenta veic pēc-incidenta pārbaudi, lai apzinātu iegūto pieredzi, trūkumus reaģēšanā uz incidentiem un uzlabošanas iespējas.

55. Informācijas fiziskās drošības pamatprasības

55.1. Informācijas fiziskās drošības aizsardzībai nodrošina piekļuves kontroles mehānismus, tajā skaitā piekļuves kartes vai atslēgas, lai ierobežotu nesankcionētu piekļuvi ēkām un telpām.

55.2. Piekļuves tiesības piešķirs atbilstoši šīs politikas 26.1. punktā noteiktajam principam.

55.3. Piekļuves kontroles sistēmas tiks regulāri uzraudzītas, uzturētas un atjauninātas, lai novērstu nesankcionētu piekļuvi.

55.4. LU ierīkos un uzturēs atbilstošas fiziskas barjeras, žogus, vārtus un barjeras, lai nodrošinātu LU ēku un teritoriju aizsardzību.

VI. Noslēguma jautājumi

56. LU informācijas drošības pārvaldības dokumentus pārskata vismaz reizi gadā un aktualizē, ja tiek konstatēta atbilstoša nepieciešamība, kā arī gadījumos:

56.1. ja izmaiņas Informācijas sistēmās var ietekmēt to drošību;

56.2. ja mainījušies vai ir atklāti jauni Informācijas sistēmu drošības apdraudējumi;

56.3. ja noticis nozīmīgs Informācijas sistēmu drošības incidents;

56.4. ja izdarīti grozījumi spēkā esošajos normatīvajos aktos, kas regulē informācijas drošību vai Informācijas sistēmu darbību.

57. Politiku aktualizē un pārskata LU Informācijas tehnoloģiju drošības pārvaldnieks un nepieciešamos grozījumus virza apstiprināšanai normatīvajos aktos noteiktā kārtībā.