APSTIPRINĀTS
ar SIA „Rīgas Austrumu klīniskā universitātes slimnīca”
padomes 2026. gada 9. aprīļa sēdes Nr. 2026-P01-9 lēmumu
(sēdes protokols Nr. 2026-P1-03-9)

SIA “Rīgas Austrumu klīniskā universitātes slimnīca” kiberdrošības politika

Saturs

I. Lietotie termini

1. Iekšējā normatīvajā aktā "SIA "Rīgas Austrumu klīniskā universitātes slimnīca" kiberdrošības politika" lietotie termini un saīsinājumi (alfabētiskā secībā):

1.1. **Autentifikācija** – process, ar kura palīdzību sistēma pārbauda lietotāja identitāti pirms piekļuves piešķiršanas Informācijas sistēmām vai resursiem.

1.2. **Autentiskums** – informācijas patiesuma apliecināšana.

1.3. **Darbinieks** – jebkura Slimnīcā uz darba līguma pamata nodarbināta fiziska persona, tajā skaitā Darbinieks, kuram noteikts valsts amatpersonas statuss, kā arī Slimnīcas valdes un padomes locekļi, kuri darbojas uz pilnvarojuma līguma pamata.

1.4. **Daudzfaktoru autentifikācija** – Autentifikācijas mehānisms, kurā tiek izmantoti vairāki faktori (ko es zinu, kas man ir, kas es esmu, vai citi).

1.5. **Fiziskā aizsardzība** – Informācijas un tehnisko resursu aizsardzība pret fiziskas iedarbības, vides vai cilvēkfaktoru radītiem bojājumiem, kas var ietekmēt to Pieejamību, Integritāti vai Konfidencialitāti.

1.6. **Ievainojamība** – informācijas un komunikācijas tehnoloģiju vai ar tām saistītu pakalpojumu vājums, nepilnība vai kļūda, kuru var izmantot kiberapdraudējums, lai iegūtu nesankcionētu piekļuvi, traucētu darbību vai apdraudētu datu drošību.

1.7. **IKT** – Informācijas un komunikācijas tehnoloģijas.

1.8. **Informācija** – datu kopums, kas nodrošina uzdevumu izpildi un lēmumu pieņemšanu neatkarīgi no tā eksistences veida, tostarp jebkurā tehniski iespējamā fiksēšanas, glabāšanas, apstrādes vai nodošanas veidā.

1.9. **Informācijas sistēma** (arī **IS**) – strukturizēts IT, programmatūras un datu bāzu kopums, kuru lietojot tiek nodrošināta noteiktu Slimnīcas funkciju izpildei nepieciešamās Informācijas ierosināšana, radīšana, apkopošana, apstrāde un glabāšana.

1.10. **Integritāte** – Informācijas resursa un tā elektroniskās apstrādes metožu precizitāte, pareizība un pilnīgums.

1.11. **IS moduļa pārzinis** – Darbinieks, kura atbildībā atrodas konkrētas IS moduļa pārvaldība Slimnīcā.

1.12. **IS pārzinis** – Darbinieks, kura atbildībā atrodas konkrētas IS pārvaldība Slimnīcā.

1.13. **IT –** Informācijas tehnoloģijas**;**

1.14. **Kiberhigiēna** – ikdienas prakse un uzvedības principi, kas samazina kiberincidentu risku (piemēram, drošu paroļu lietošana, programmatūras atjaunināšana).

1.15. **Kiberdrošības pārvaldnieks –** Slimnīcas IT drošības vadītājs – Darbinieks, kurš īsteno un pārrauga Slimnīcas kiberdrošības pasākumus.

1.16. **Kiberdrošības incidents** (arī **Kiberincidents**) – notikums, kas apdraud apstrādātu datus vai tādu pakalpojumu pieejamību, Autentiskumu, Integritāti vai Konfidencialitāti, kurus piedāvā tīklu un IS vai kuri pieejami ar tīklu un IS starpniecību.

1.17. **Kiberdrošības riski** (arī **Kiberriski**) – draudi un iespējamie zaudējumi, kas var rasties Slimnīcai IKT un IS izmantošanas dēļ.

1.18. **Kiberincidentu žurnāls** – Kiberdrošības pārvaldnieka uzturēts Kiberdrošības incidentu reģistrs, kas ietver informāciju par notikumu, tā analīzi, veiktajām reaģēšanas darbībām un pieņemtajiem lēmumiem.

1.19. **Konfidencialitāte** – piekļuve IS tikai pilnvarotiem IKT procesiem un lietotājiem.

1.20. **Lietotāja konts** – konts, kas ir piesaistīts konkrētam Lietotājam.

1.21. **Lietotājs** – persona, kurai ir piešķirtas tiesības lietot IS vai TR.

1.22. **Loģiskā aizsardzība** – IS aizsardzība, kuru realizē ar programmatūras līdzekļiem.

1.23. **Nepārtrauktības plāns** –pasākumu kopums, kas nosaka, kā Slimnīca uzturēs IKT un atjaunos savu darbību gadījumā, ja notiks Kiberincidents.

1.24. **NKDL** – Nacionālās kiberdrošības likums.

1.25. **Pieejamība** – iespēja Lietotājam lietot IS vai Informācijas resursu noteiktā laikā un vietā.

1.26. **Politika** – Slimnīcas iekšējais normatīvais akts "Kiberdrošības politika".

1.27. **SAB –** Satversmes aizsardzības birojs, kas ir Latvijas valsts drošības iestāde, kuras galvenie uzdevumi ir izlūkošana, pretizlūkošana un valsts noslēpuma aizsardzība.

1.28. **Slimnīca -** SIA "Rīgas Austrumu klīniskā universitātes slimnīca", kura ir publiskas personas kapitālsabiedrība, kuras 100% valsts kapitālu daļu turētājs ir Latvijas Republikas Veselības ministrija.

1.29. **Tehniskais resurss** (arī **TR**) – aparatūra, iekārta, kas ir tīkla vai IS sastāvdaļa vai IKT infrastruktūrā izmantota iekārta, kas veic datu apmaiņu ar IS, un programmatūra, tostarp operētājsistēmas, sistēmfaili, sistēmprogrammas, lietojumprogrammas un palīgprogrammas.

1.30. **TR pārzinis** – Darbinieks, kura atbildībā atrodas konkrēta TR pārvaldība Slimnīcā.

1.31. **VDAR** – Eiropas Savienības Vispārīgā datu aizsardzības regula *(General Data Protection Regulation)*, kas nosaka prasības personas datu aizsardzībai (Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK.

2. Citi Politikā lietotie termini ir skaidrojami atbilstoši tam, kā tie ir definēti NKDL un Ministru kabineta 2025. gada 25. jūnija noteikumos Nr. 397 "Minimālās kiberdrošības prasības".

II. Vispārējie noteikumi

3. Politika nosaka kiberdrošības pārvaldības struktūru, lomu un atbildības sadalījumu principus un pamatprasības, kas jāievēro, lai nodrošinātu atbilstības un darbības nepārtrauktības nodrošināšanu, lai nodrošinātu drošu un nepārtrauktu Slimnīcas IKT sistēmu un IS resursu pārvaldību atbilstoši Latvijas Republikas normatīvajiem aktiem un starptautiskajai labajai praksei.

4. Politikas mērķis ir mazināt Kiberdrošības incidentu iespējamību, nodrošinot Slimnīcas resursu drošību, Konfidencialitāti, Integritāti, Pieejamību un Autentiskumu, kā arī veicināt Darbinieku izpratni par kiberdrošības nozīmi.

5. Kiberdrošības mērķi ietver četrus informācijas drošības pamatprincipus:

5.1. Konfidencialitāte – nodrošināt, ka informācija ir pieejama tikai autorizētiem lietotājiem;

5.2. Integritāte – nodrošināt informācijas precizitāti, pilnīgumu un aizsardzību pret neatļautām izmaiņām;

5.3. Pieejamība – nodrošināt autorizētu lietotāju piekļuvi informācijai un IKT resursiem atbilstoši noteiktajām prasībām;

5.4. Autentiskums – nodrošināt, ka informācijas avots un saņēmējs ir autentificēti, pārbaudāmi un uzticami.

III. Slimnīcas vispārīgs raksturojums, darbības jomas un sniegtie pakalpojumi

6. Slimnīcas darbības joma ir veselības aprūpes pakalpojumu sniegšana, zinātniskās darbības veikšana un mācību procesa nodrošināšana.

7. Slimnīca klasificējas kā kritiskās infrastruktūras un būtisko pakalpojumu sniedzējs atbilstoši NKDL prasībām, kas uzliek pienākumu ievērot īpašas kiberdrošības pārvaldības prasības un ziņošanas pienākumus par nozīmīgiem Kiberincidentiem kompetentajām institūcijām.

IV. Kiberdrošības politikas uzdevumi un piemērojamība

8. Politika nosaka kiberdrošības pārvaldības vispārējos principus, atbildības jomas un prasības Slimnīcas struktūrvienībām un Darbiniekiem, kā arī paredz informēšanas un apmācību pasākumus kiberdrošības kultūras veidošanai.

9. Politikas uzdevumi:

9.1. lai sasniegtu Politikas mērķus un nodrošinātu Slimnīcas IS un informācijas resursu aizsardzību atbilstoši normatīvajiem aktiem un starptautiskajai praksei, šī Politika nosaka šādus uzdevumus:

9.1.1. noteikt kiberdrošības pārvaldības struktūru un atbildības sadalījumu Slimnīcā;

9.1.2. nodrošināt atbilstību normatīvajiem aktiem un starptautiskajiem standartiem;

9.1.3. samazināt Kiberincidentu risku, ieviešot drošības pasākumus;

9.1.4. ievērot informācijas drošības pamatprincipus – Konfidencialitāti, Integritāti, Pieejamību un Autentiskumu;

9.1.5. veicināt Darbinieku izpratni un Kiberhigiēnu;

9.1.6. noteikt Slimnīcas struktūrvienību un Lietotāju pienākumus kiberdrošībā;

9.1.7. pārvaldīt Kiberriskus, nodrošinot to identificēšanu, novērtēšanu un mazināšanu.

10. Politikas tvērums un piemērojamība:

10.1. Politika ir saistoša visiem Slimnīcas Darbiniekiem, līgumdarbiniekiem, praktikantiem, rezidentiem, ārpakalpojumu sniedzējiem, sadarbības partneriem un citām personām, kurām piešķirtas tiesības piekļūt Slimnīcas IS vai IKT resursiem;

10.2. Politikas prasības ir attiecināmas uz visu Slimnīcas rīcībā esošo informāciju, neatkarīgi no tās apstrādes, glabāšanas vai pārsūtīšanas veida un izmantotajiem tehnoloģiskajiem resursiem;

10.3. Politikas izpilde ir obligāta visās Slimnīcas struktūrvienībās un visos informācijas tehnoloģiju procesos, kas saistīti ar IKT resursu izmantošanu, attīstību un uzturēšanu.

11. Politika ir izstrādāta, ievērojot Latvijas Republikas un Eiropas Savienības normatīvos aktus, kā arī starptautiskos standartus kiberdrošības jomā, īpaši:

11.1. NKDL;

11.2. Ministru kabineta noteikumus, kas izdoti uz NKDL pamata;

11.3. citus normatīvos aktus un standartus, tostarp Eiropas Savienības normatīvos aktus un starptautiskos standartus, kas attiecas uz veselības aprūpes pakalpojumu sniegšanu;

11.4. VDAR;

11.5. Starptautiskos drošības standartus.

V. Kiberdrošības pārvaldības struktūra

12. Slimnīcas kiberdrošības pārvaldības struktūra ir izveidota tā, lai skaidri noteiktu atbildības jomas, nodrošinātu efektīvu komunikāciju starp dažādām Slimnīcas struktūrvienībām un veicinātu sadarbību ar ārējām institūcijām kiberdrošības jautājumos.

13. Kiberdrošības pārvaldības struktūru veido šādas galvenās atbildīgās puses:

13.1. Slimnīcas padome – apstiprina Politiku un uzrauga tās īstenošanu;

13.2. Slimnīcas valde:

13.2.1. uzrauga ārējo normatīvo aktu kiberdrošības prasību ieviešanu Slimnīcā;

13.2.2. apstiprina Politiku (virzīšanai apstiprināšanai padomei) un citus ar kiberdrošību saistītos iekšējos normatīvos aktus;

13.2.3. nodrošina nepieciešamo resursu piešķiršanu kiberdrošībai;

13.2.4. regulāri pārskata kiberdrošības pārvaldības efektivitāti Slimnīcā, analizē Kiberdrošības pārvaldnieka sagatavotos ziņojumus par incidentiem, risku novērtējumiem un citiem būtiskiem jautājumiem, kā arī pieņem lēmumus par kiberdrošības pasākumu uzlabošanu;

13.2.5. nosaka Kiberdrošības pārvaldnieku;

13.2.6. nodrošina Kiberdrošības pārvaldības funkciju nepārtrauktību, nosakot Kiberdrošības pārvaldnieka aizvietošanas kārtību viņa prombūtnes laikā;

13.2.7. nodrošina Kiberdrošības risku pārvaldību atbilstoši Slimnīcasdarbības kritiskumam un pieejamajiem finanšu, cilvēkresursiem un tehniskajiem resursiem, prioritizējot pacientu drošību un būtisko pakalpojumu nepārtrauktību;

13.2.8. gadījumos, kad normatīvo aktu prasību pilnīga ieviešana nav iespējama resursu ierobežojumu dēļ, tiek dokumentēti pieņemtie lēmumi, identificētie riski un izvēlētie kompensējošie pasākumi.

13.3. Kiberdrošības pārvaldnieks, kura galvenie uzdevumi ir:

13.3.1. nodrošināt Politikas īstenošanu un aktualizēšanu atbilstoši normatīvo aktu prasībām;

13.3.2. izstrādāt, uzturēt un regulāri pārskatīt Slimnīcas kiberdrošības iekšējo dokumentāciju;

13.3.3. izstrādāt, uzturēt un regulāri aktualizēt Slimnīcas darbības nepārtrauktības plānu valsts apdraudējuma gadījumam, nodrošinot tā saskaņotību ar citiem darbības nepārtrauktības un civilās aizsardzības dokumentiem;

13.3.4. organizēt un koordinēt regulārus Kiberdrošības risku novērtējumus un auditus;

13.3.5. vadīt un koordinēt Kiberincidentu pārvaldību, tai skaitā incidentu identificēšanu, izmeklēšanu un seku novēršanu, kā arī Kiberincidentu žurnāla uzturēšanu;

13.3.6. sagatavot ziņojumus Slimnīcas valdei par kiberdrošības situāciju, incidentiem un riskiem;

13.3.7. organizēt un koordinēt Darbinieku kiberdrošības apmācības un informēšanas pasākumus;

13.3.8. sadarboties ar ārējām kiberdrošības institūcijām (CERT.LV, SAB, Nacionālais kiberdrošības centrs);

13.3.9. sadarboties ar Slimnīcas datu aizsardzības speciālistu, nodrošinot personas datu drošības risku identificēšanu un atbilstību VDAR prasībām.

13.4. IS pārziņi, kuri ir atbildīgi par:

13.4.1. IS klasifikāciju pēc Konfidencialitātes, Integritātes un Pieejamības principiem;

13.4.2. Lietotāju piekļuves tiesību pieprasīšanas, piešķiršanas un regulāras pārskatīšanas organizēšanu;

13.4.3. sadarbību ar Kiberdrošības pārvaldnieku Kiberrisku novērtēšanā attiecībā uz Informācijas saturu un tā apstrādes drošību;

13.4.4. sadarbību ar IT struktūrvienībām un Kiberdrošības pārvaldnieku attiecībā uz datu aizsardzības, glabāšanas un pieejamības jautājumiem.

13.5. TR pārziņi, kuri ir atbildīgi par:

13.5.1. TR konfigurāciju, atjauninājumu uzstādīšanu un darbspējas nodrošināšanu;

13.5.2. rezerves kopiju veidošanu, glabāšanu un datu atjaunošanas procesu organizēšanu;

13.5.3. drošības prasību ieviešanu un uzraudzību saistībā ar infrastruktūru, tīklu iekārtām, serveriem un lietojumu vidēm;

13.5.4. sadarbību ar Kiberdrošības pārvaldnieku TR izvērtēšanā un drošības incidentu izmeklēšanā un seku novēršanā.

13.6. Slimnīcas struktūrvienību vadītāji ir atbildīgi, ka tās Darbinieki ievēro Politikas principus un prasības, un viņiem ir šādi pienākumi:

13.6.1. nodrošināt, ka viņu padotībā esošie Darbinieki ir informēti par kiberdrošības prasībām un ievēro tās;

13.6.2. pārskatīt Darbinieku piešķirtās piekļuves tiesības un ziņot IT struktūrvienībai vai atbildīgo resursu pārziņus par nepieciešamajām izmaiņām;

13.6.3. nekavējoties ziņot Kiberdrošības pārvaldniekam par iespējamiem vai notikušiem Kiberincidentiem, pārkāpumiem un drošības riskiem;

13.6.4. nodrošināt struktūrvienības Darbinieku dalību kiberdrošības apmācībās un informēšanas pasākumos.

13.7. Darbiniekiem un IS Lietotājiem, ir šādi pienākumi:

13.7.1. iepazīties ar Politiku un saistītajiem normatīvajiem dokumentiem, kā arī ievērot tos;

13.7.2. izmantot Slimnīcas IS un resursus tikai darba pienākumu izpildei, ievērojot piešķirtās piekļuves tiesības un drošības prasības;

13.7.3. nekavējoties informēt Kiberdrošības pārvaldnieku vai IT struktūrvienības par aizdomīgiem e-pastiem, incidentiem, neatļautām darbībām vai jebkuru citu Kiberincidenta pazīmi;

13.7.4. neizpaust Lietotāja konta informāciju citām personām;

13.7.5. piedalīties Slimnīcas organizētajās kiberdrošības apmācībās.

13.8. IT struktūrvienības un tehniskā atbalsta personāls ir atbildīgs par:

13.8.1. Slimnīcas IT infrastruktūras drošu uzturēšanu un sistēmu darbspēju;

13.8.2. drošības ielāpu, programmatūras un sistēmu atjauninājumu savlaicīgu ieviešanu;

13.8.3. Kiberincidentu sākotnējo reģistrēšanu un nodošanu Kiberdrošības pārvaldniekam turpmākai izmeklēšanai;

13.8.4. sadarbību Kiberincidentu seku novēršanā un sistēmu atjaunošanā.

14. Slimnīca nepieciešamības gadījumā sadarbojas ar ārējām kiberdrošības institūcijām, tostarp CERT.LV, SAB un Nacionālo kiberdrošības centru, lai saņemtu un sniegtu informāciju par iespējamiem draudiem un Kiberincidentiem, kā arī dalītos pieredzē un iegūtu nepieciešamo atbalstu Kiberincidentu pārvaldībā.

15. Kiberdrošības pārvaldnieks nodrošina operatīvu informācijas apmaiņu un incidentu ziņošanu CERT.LV un SAB atbilstoši iekšējiem normatīvajiem aktiem.

16. Kiberincidenta gadījumā Slimnīca nodrošina incidenta izvērtēšanu iespējami īsā laikā pēc tā konstatēšanas.

17. Lēmumu par Kiberincidenta būtiskumu un ziņošanu kompetentajām iestādēm pieņem Kiberdrošības pārvaldnieks sadarbībā ar Slimnīcas valdi, ņemot vērā piemērojamos normatīvos aktus, incidenta ietekmi uz informācijas un pacientu drošību un Slimnīcas operatīvās darbības nepārtrauktību.

18. Kiberdrošības pārvaldnieks koordinē iekšējo Kiberincidentu pārvaldību, nodrošinot efektīvu sadarbību starp IT struktūrvienībām, IS pārziņiem un TR pārziņiem, kā arī Slimnīcas vadību incidentu identificēšanas, novēršanas un seku mazināšanas procesā.

19. Nepieciešamības gadījumā Slimnīca var iesaistīt ārējos kiberdrošības ekspertus vai konsultantus, lai veiktu neatkarīgu auditu vai sniegtu atbalstu īpaši sarežģītu Kiberincidentu novēršanā un izmeklēšanā.

VI. Kiberapdraudējumu veidi un to ietekme uz Slimnīcas darbību

20. Slimnīcas darbības nodrošināšanai tiek izmantoti IKT un IS, kuru ietvaros tiek apstrādāta un uzturēta šāda informācija:

20.1. pacientu personas dati, tai skaitā īpaši aizsargājamie personas dati par veselību, kas iegūti ārstniecības procesā un veselības aprūpes pakalpojumu nodrošināšanas ietvaros;

20.2. informācija par ārstniecības iestādes telpu plānojumu, inženiertehniskajām komunikācijām un medicīnisko tehnoloģiju izvietojumu;

20.3. finanšu dati par Slimnīcas norēķiniem ar pacientiem, valsts un pašvaldību institūcijām, apdrošinātājiem un pakalpojumu sniedzējiem;

20.4. ārpakalpojumu sniedzēju līgumi un informācija par šo līgumu izpildi;

20.5. personāla dati, tai skaitā informācija par nodarbinātības attiecībām un piekļuvi Slimnīcas Informācijas sistēmām;

20.6. informācija par IKT infrastruktūru, tai skaitā serveriem, tīkla iekārtām, medicīnas Informācijas sistēmām un specializētām ārstniecības iekārtu vadības sistēmām;

20.7. cita informācija.

21. Kiberuzbrukumu gadījumā var tikt būtiski ietekmēti šādi Slimnīcas procesi:

21.1. ārstniecības pakalpojumu nepārtrauktība un pacientu dzīvības un veselības drošība, tai skaitā situācijās, kad tiek traucēta dzīvību uzturošu medicīnisko iekārtu, diagnostikas vai operāciju bloka sistēmu darbība;

21.2. medicīnisko ierakstu, izmeklējumu un citu pacientu datu pieejamība un precizitāte, kas var ietekmēt ārstniecības lēmumu pieņemšanu;

21.3. resursu, telpu, medicīnisko iekārtu un personāla piekļuves un drošības kontrole, tai skaitā pacientu drošas uzturēšanās nodrošināšana ārstniecības iestādē;

21.4. finanšu norēķinu, uzskaites un līgumu izpildes sistēmu darbība;

21.5. administratīvo, atbalsta un vadības funkciju (piemēram, personāla, dokumentu un iekšējās komunikācijas) nodrošināšana;

21.6. ārējā komunikācija ar valsts institūcijām, sadarbības partneriem un sabiedrību, kas var ietekmēt Slimnīcas reputāciju un sabiedrības uzticību veselības aprūpes sistēmai;

21.7. citi procesi.

22. Slimnīca aizsargā gan iekšējos, gan ārējos IKT resursus no kiberuzbrukumiem, izmantojot organizatoriskos, tehniskos un cilvēkresursu aizsardzības pasākumus, tostarp drošības politikas, piekļuves kontroles, rezerves kopijas, incidentu vadības procedūras un personāla izglītošanu.

23. Slimnīcas ārējos IKT resursus apdraud šādi nozīmīgākie kiberapdraudējumu veidi:

23.1. pakalpojumu atteices (DoS un DDoS) uzbrukumi, kas var traucēt Slimnīcas tīmekļvietņu, e-pakalpojumu un komunikācijas sistēmu darbību;

23.2. ielaušanās mēģinājumi tīmekļvietnēs vai publiski pieejamās sistēmās, tostarp izmantojot Ievainojamības, nepareizu konfigurāciju vai novecojušu programmatūru;

23.3. datu eksfiltrācija vai zādzība, izmantojot tīmekļa Ievainojamības vai ļaunprātīgus pielikumus.

24. Slimnīcas iekšējos IKT resursus apdraud šādi nozīmīgākie kiberapdraudējumu veidi:

24.1. pikšķerēšanas uzbrukumi un sociālās inženierijas paņēmieni, kas vērsti uz Darbinieku apmānīšanu vai piekļuves datu iegūšanu;

24.2. šifrējošo izspiedējvīrusu (*ransomware*) uzbrukumi, kas var paralizēt sistēmu darbību un apdraudēt pacientu datu pieejamību;

24.3. nejauši datu zudumi, cilvēkfaktora kļūdas vai Darbinieku/ārpakalpojumu sniedzēju prettiesiskas darbības;

24.4. neatjauninātas vai neatbalstītas programmatūras izmantošana, kas rada Ievainojamību;

24.5. iekšēji ielaušanās mēģinājumi vai ļaunprātīga piekļuve sistēmām, kas var būt saistīta ar nepareizu piekļuves tiesību pārvaldību vai drošības kontroles apiešanu.

VII. IS un IKT resursu pārvaldība

25. Slimnīca uztur vienotu, aktualizētu un detalizētu IKT resursu un IS katalogu. Katalogs ietver resursu nosaukumus, atbildīgās personas (resursu pārziņus), informācijas klasifikācijas līmeni, atrašanās vietu, kā arī citas būtiskas tehniskās un organizatoriskās īpašības.

26. Katalogu uztur IT struktūrvienības sadarbībā ar IS un IKT resursu pārziņiem un Kiberdrošības pārvaldnieku, aktualizējot informāciju vismaz reizi gadā vai pēc būtiskām izmaiņām.

27. Slimnīca nodrošina IKT resursu dzīves cikla pārvaldību — sākot no to iegādes, ieviešanas un ekspluatācijas līdz utilizācijai, ievērojot datu drošības un konfidencialitātes prasības visos posmos.

28. Slimnīcā visas IS tiek klasificētas pēc Konfidencialitātes, Integritātes un Pieejamības līmeņiem, ievērojot risku novērtējumu un normatīvo aktu prasības.

29. Klasifikācija tiek veikta vismaz reizi gadā, un atbildība par klasifikāciju ir IS pārziņiem sadarbībā ar Kiberdrošības pārvaldnieku.

30. Klasifikācijas rezultāti tiek izmantoti, lai noteiktu prioritātes un nepieciešamos, piemērotos drošības pasākumus resursu aizsardzībā un Kiberincidentu pārvaldībā.

31. Slimnīca izvērtē Kiberdrošības riskus attiecībā uz kritiskajiem ārpakalpojumu sniedzējiem un piegādātājiem proporcionāli pakalpojuma nozīmīgumam.

32. Slimnīca atbilstoši iespējām nosaka minimālās drošības prasības ārpakalpojumu sniedzējiem un piegādātājiem, tostarp piekļuves ierobežošanu un informēšanas pienākumu Kiberincidentu gadījumā, ciktāl tas ir iespējams.

33. Pieejas tiesības Slimnīcas Informācijas resursiem un IS tiek piešķirtas pēc principa „nepieciešamība zināt" – Lietotājiem tiek piešķirtas tikai tās tiesības, kas ir nepieciešamas tiešo darba pienākumu izpildei.

34. Ja piekļuvi Slimnīcas IS vai IKT resursiem nepieciešams nodrošināt ārējiem piegādātājiem, uzturētājiem vai pakalpojumu sniedzējiem, šāda piekļuve tiek piešķirta tikai uz līguma pamata, ar noteiktiem drošības nosacījumiem un laika ierobežojumiem, ievērojot Slimnīcas datu aizsardzības prasības.

35. Pieejas tiesību pieprasījums, piešķiršana, grozīšana un anulēšana tiek veikta atbilstoši Slimnīcas resursu pieprasīšanas procesam.

36. Reizi gadā Kiberdrošības pārvaldnieks sadarbībā ar IS pārziņiem veic Lietotāju piekļuves tiesību pārskatīšanu un nepieciešamās korekcijas.

37. Slimnīcas atbildīgās struktūrvienības atbilstoši kompetencei (IT, Drošības konsultants, utt.) nodrošina Lietotāju veikto aktivitāšu uzskaiti žurnālfailos notikumu izsekojamībai un drošības incidentu izmeklējamībai.

38. Slimnīca izmanto Daudzfaktoru autentifikāciju (MFA), t.sk. attālinātai piekļuvei Slimnīcas iekšējiem tīkliem.

39. Autentifikācijas prasības regulāri pārskata Kiberdrošības pārvaldnieks un IT struktūrvienības atbilstoši aktuālajiem Kiberdrošības riskiem un tehnoloģiskajām iespējām.

40. Atbildīgās struktūrvienības (IT, Drošības konsultants, Tehnisko sistēmu nodrošinājuma, drošības un transporta daļa, utt.) nodrošina atbilstošus Fiziskās aizsardzības pasākumus serveru telpām un kritiskajiem IKT resursiem, piemēram, piekļuves kontroli, videonovērošanu, klimata kontroli, nepārtrauktu elektroenerģijas padevi (UPS), ugunsdrošības pasākumus u.c.

41. IT struktūrvienības nosaka drošības prasības pārnēsājamo ierīču, datu nesēju un klēpjdatoru lietošanai, tai skaitā datu šifrēšanu, piekļuves kontroli un ierīču uzskaiti.

42. IT struktūrvienības resursu Loģisko aizsardzību nodrošina ar ugunsmūra risinājumu, regulārām drošības pārbaudēm, Ievainojamību skenēšanu un nepieciešamības gadījumā — ielaušanās testiem, kā arī regulāriem programmatūras un sistēmu atjauninājumiem un žurnālfailu pierakstu uzraudzību.

43. IT struktūrvienības nodrošina būtisko datu un IS rezerves kopiju veidošanu, atbilstoši definētiem intervāliem un kritiskuma līmeņiem, lai nodrošinātu iespēju atjaunot datus un IS darbību incidentu vai datu zuduma gadījumā.

44. IT struktūrvienības nodrošina, ka jaunas programmatūras vai IS moduļu ieviešana, kā arī būtiski atjauninājumi tiek veikti tikai pēc saskaņotas izmaiņu pārvaldības procedūras, ietverot drošības testēšanu, ietekmes novērtējumu un atbildīgo personu apstiprinājumu.

45. IT struktūrvienības nodrošina rezerves kopiju uzglabāšanu un veic datu atjaunošanas testēšanas procedūras.

46. Slimnīca izmanto tikai licencētu programmatūru, ievērojot licenču lietošanas noteikumus un nodrošinot nepieciešamo atbilstību autortiesībām un normatīvajiem aktiem.

47. IT struktūrvienības uztur centralizētu programmatūras uzskaiti un veic regulāru programmatūras atjauninājumu instalēšanu un drošības ielāpu uzstādīšanu, nodrošinot programmatūras drošības prasību ievērošanu.

48. Kiberdrošības pārvaldnieks sadarbībā ar IT struktūrvienībām izvērtē programmatūras ievainojamības un veic nepieciešamos pasākumus, lai novērstu drošības riskus, kas saistīti ar novecojušu vai ievainojamu programmatūru.

VIII. IKT darbības nepārtrauktības nodrošināšana

49. Slimnīca īsteno sistemātisku pieeju IKT darbības nepārtrauktības plānošanā, lai nodrošinātu kritisko pakalpojumu un funkciju atjaunošanu pēc iespējamiem incidentiem vai ārkārtas situācijām.

50. Nepārtrauktības plānošana tiek balstīta uz risku novērtējumu un IS resursu klasifikācijas rezultātiem, definējot pieļaujamos atjaunošanas laika mērķus (*Recovery Time Objective* - RTO) un atjaunošanas punkta mērķus (*Recovery Point Objective* - RPO) katram kritiskajam resursam vai pakalpojumam.

51. Nepārtrauktības plānā ietvertie pasākumi tiek savlaicīgi ieviesti, nosakot konkrētas atbildības, uzdevumus, termiņus un nepieciešamos resursus šo pasākumu īstenošanai. Nepārtrauktības plānā tiek ietverti:

51.1. rīcības scenāriji gadījumiem, ja esošie risku pārvaldības pasākumi jebkādu apstākļu dēļ ir kļuvuši nepietiekami un kādi no nepieciešamajiem resursiem IS darbības nodrošināšanai nav pieejami;

51.2. pasākumu apraksti IS darbības atjaunošanai ārkārtas situācijā;

51.3. rīcības scenāriji valsts apdraudējuma, Kiberincidentu, plaša mēroga infrastruktūras bojājumu vai citu krīzes situāciju gadījumos, nodrošinot Slimnīcas spēju turpināt būtisko pakalpojumu sniegšanu minimālā apjomā.

52. Kiberdrošības pārvaldnieks vismaz reizi gadā vai pēc būtiskām izmaiņām pārskata un aktualizē Nepārtrauktības plānu, nodrošinot tā atbilstību aktuālajiem draudiem, tehnoloģijām, kā arī izmaiņām Slimnīcas darbības procesos un infrastruktūrā. Kiberdrošības pārvaldnieks Nepārtrauktības plāna aktualizēšanā iesaista šādas atbildīgās puses:

52.1. IT struktūrvienības;

52.2. IS un IKT resursu pārziņus;

52.3. struktūrvienību vadītājus;

52.4. risku un pacientu drošības vadītāju.

53. Nepārtrauktības plānu apstiprina Slimnīcas valde.

54. Nepārtrauktības plāns tiek saskaņots ar Slimnīcas civilās aizsardzības plānu un katastrofu pārvaldīšanas dokumentiem, nodrošinot vienotu pieeju ārkārtas situāciju pārvaldībai.

55. IKT darbības nepārtrauktības pārvaldīšanas ietvaros IS pārziņi, IS moduļu pārziņi un TR pārziņi sadarbībā ar Kiberdrošības pārvaldnieku veic šādus pasākumus:

55.1. identificē visus TR, kas nodrošina konkrētas IS darbību;

55.2. nosaka prioritātes līmeņus atjaunojamajām IS atkarībā no to svarīguma Slimnīcas funkciju veikšanai;

55.3. definē veicamās procedūras IS un TR atjaunošanai;

55.4. vismaz vienu reizi gadā organizē darbības nepārtrauktības plānu testēšanu, kuras laikā tiek dokumentēti veiktie pasākumi, to rezultāti, atklātās nepilnības un turpmāk veicamie pasākumi nepilnību novēršanai.

56. IT struktūrvienības nodrošina, ka:

56.1. tiek uzturēti TR rezerves un alternatīvi pieslēgumi (tīkla savienojumi, rezerves serveri, datu glabāšanas vietas), kas nepieciešami kritisko IS un pakalpojumu nepārtrauktas darbības nodrošināšanai Kiberincidentu vai ārkārtas situāciju gadījumā;

56.2. rezerves resursu un pieslēgumu konfigurācija tiek pārbaudīta un testēta, lai pārliecinātos par to efektivitāti un gatavību nodrošināt nepārtrauktu IS darbību ārkārtas situācijās;

56.3. testēšanas rezultāti tiek dokumentēti, analizēti, un nepieciešamie pilnveidošanas pasākumi tiek iekļauti atjauninātajā Nepārtrauktības plānā un Kiberrisku reģistrā, par ko tiek informēta Slimnīcas valde;

56.4. Nepārtrauktības plāna testēšana tiek veikta vismaz reizi gadā, pārbaudot plānā ietverto pasākumu efektivitāti, spēju atjaunot sistēmu darbību un datu pieejamību plānotajos atjaunošanas laikos, kā arī nodrošina regulāras apmācības un praktiskās mācības par rīcību ārkārtas un valsts apdraudējuma gadījumos, lai pārbaudītu Slimnīcas gatavību īstenot nepārtrauktības pasākumus;

57. Kiberdrošības pārvaldnieks sadarbībā ar 52. punktā minētajām personām nodrošina Nepārtrauktības plāna regulāru aktualizēšanu un pārskatīšanu, kā arī informē Darbiniekus un atbildīgās personas par nepārtrauktības pasākumiem un rīcību incidentu gadījumos.

IX. Kiberdrošības risku pārvaldība

58. Slimnīcā Kiberrisku pārvaldība tiek īstenota, ievērojot starptautiski atzītu kiberrisku vadības metodoloģiju.

59. Kiberrisku pārvaldības procesā tiek identificēti, analizēti, novērtēti un uzraudzīti Kiberriski, izvērtējot draudu avotus, sistēmu Ievainojamības, iespējamo ietekmi un Kiberincidentu varbūtību.

60. Kiberrisku novērtēšana tiek veikta vismaz reizi gadā vai pēc būtiskām izmaiņām IS vai IKT resursu konfigurācijā, kā arī pēc nozīmīgu Kiberincidentu iestāšanās.

61. Novērtēšanas procesā tiek identificēti esošie un jaunie Kiberriski, noteikta to ietekme uz Slimnīcas darbību un resursiem, kā arī analizēta risku iespējamība un potenciālās sekas.

62. Kiberrisku uzraudzību veic Kiberdrošības pārvaldnieks sadarbībā ar IS un IKT resursu pārziņiem, atjauninot risku novērtējumu un nepieciešamos aizsardzības pasākumus, par ko tiek informēta Slimnīcas valde.

63. Pamatojoties uz Kiberrisku novērtēšanas rezultātiem, tiek plānoti un ieviesti konkrēti Kiberrisku mazināšanas pasākumi, kuru mērķis ir samazināt risku iestāšanās varbūtību vai negatīvās sekas. Kiberrisku mazināšanas pasākumi tiek apkopoti Kiberrisku mazināšanas plānā.

64. Kiberdrošības pārvaldnieks nodrošina Kiberrisku mazināšanas plāna izpildes kontroli un ziņo par šī plāna izpildes gaitu Slimnīcas valdei.

65. Kiberdrošības pārvaldnieks uztur Kiberrisku reģistru, kurā tiek uzskaitīti visi identificētie Kiberriski, to novērtējums, potenciālā ietekme, mazināšanas pasākumi, kā arī šo pasākumu izpildes statuss.

66. Kiberrisku reģistrs tiek aktualizēts vismaz reizi gadā vai pēc būtiskām izmaiņām Slimnīcas IS un IKT infrastruktūrā, kā arī pēc Kiberincidentiem, kas var ietekmēt risku līmeni.

67. Kiberdrošības pārvaldnieks pārskata Kiberrisku reģistru kopā ar IT struktūrvienībām, IS pārziņiem un TR pārziņiem, nepieciešamības gadījumā veicot izmaiņas, par ko tiek informēta Slimnīcas valde.

68. Pamatojoties uz Kiberrisku novērtējuma rezultātiem, Kiberdrošības pārvaldnieks izstrādā un uztur Nepārtrauktības plānu valsts apdraudējuma, kiberuzbrukuma vai būtisku pakalpojumu darbības traucējumu gadījumam, nodrošinot tā pārskatīšanu un saskaņošanu ar civilās aizsardzības un katastrofu pārvaldīšanas dokumentiem.

X. Kiberhigiēnas un Darbinieku izglītošanas pasākumi

69. Katram jaunajam Darbiniekam, līgumdarbiniekam vai praktikantam, kam tiek piešķirtas piekļuves tiesības Slimnīcas IS un resursiem, tiek nodrošināta sākotnējā kiberdrošības instruktāža.

70. Sākotnējā instruktāža ietver iepazīstināšanu ar Politiku, IKT resursu lietošanas noteikumiem, pamata drošības prasībām un rīcību Kiberincidentu gadījumā.

71. Instruktāžu organizē un dokumentē Slimnīcas personāla vadība sadarbībā ar Kiberdrošības pārvaldnieku.

72. Kiberdrošības pārvaldnieks vismaz reizi gadā vai biežāk, atkarībā no aktuālajiem riskiem, Kiberincidentiem vai izmaiņām normatīvajos aktos un tehnoloģiju vidē, nodrošina kiberdrošības apmācības visiem Darbiniekiem, kuriem ir pieeja IS un IKT resursiem, lai veicinātu Darbinieku izpratni par aktuālajiem Kiberriskiem un labu praksi drošā darba veikšanai.

73. Personāla vadība un Profesionālās tālākizglītības centru "Aslimnīcas Mācību centrs" sadarbībā ar Kiberdrošības pārvaldnieku īsteno informatīvas aktivitātes un kampaņas, lai stiprinātu Darbinieku izpratni par kiberdrošību, veicinātu kiberdrošības kultūras attīstību un Darbinieku aktīvu līdzdalību Kiberrisku novēršanā.

74. Kiberdrošības kultūras veicināšanas pasākumos tiek izmantotas dažādas komunikācijas formas, piemēram, informatīvi ziņojumi iekšējā tīmekļa vietnē, e-pasta kampaņas, plakāti, interaktīvi semināri u.c.

75. Kiberdrošības pārvaldnieks nodrošina, ka Kiberhigiēnas un Darbinieku izglītošanas pasākumi tiek pielāgoti arī darbībai valsts apdraudējuma vai ārkārtas situācijās, iekļaujot tos Nepārtrauktības plānā.

XI. Noslēguma noteikumi

76. Politika stājas spēkā nākamajā darba dienā pēc tam, kad to apstiprinājusi Slimnīcas padome.

77. Politika tiek publicēta Slimnīcas iekšējā tīmekļa vietnē https://intranet.aslimnica.lv/ un Slimnīcas tīmekļa vietnē www.aslimnica.lv.

78. Darbinieki tiek iepazīstināti ar Politiku ne vēlāk kā mēneša laikā no tās apstiprināšanas. Darbinieks, kas tiek pieņemts darbā vai uzsāk amata pienākumu izpildi Slimnīcā pēc Politikas spēkā stāšanās dienas, tiek iepazīstināts ar Politiku pēc līgumisko attiecību noslēgšanas.

79. Politiku regulāri pārskata un aktualizē vismaz reizi trijos gados vai biežāk, ja tiek konstatētas būtiskas izmaiņas normatīvajos aktos, Slimnīcas darbības specifikā, izmantotajās tehnoloģijās vai pēc nozīmīgu Kiberincidentu iestāšanās.

80. Par Politikas pārskatīšanu un aktualizēšanu ir atbildīgs Slimnīcas IT direktors.