Konsolidētā versija
dokumentam ir informatīvs raksturs

Rīgas Tehniskās universitātes Informācijas un komunikācijas tehnoloģiju sistēmu drošības politika apstiprināta Senāta 2016. gada 27. jūnija Senāta sēdē (protokols Nr.601), ar grozījumiem:

- 2021. gada 27. decembrī (stājušies spēkā 28.12.2021.)

Rīgas Tehniskās universitātes informācijas un komunikācijas tehnoloģiju sistēmu drošības politika

Izdota pamatojoties uz RTU Senāta 28.04.2014. lēmuma "Rīgas Tehniskās universitātes drošības politika" (protokols Nr.580) 6.2.apakšpunktu

I. Vispārīgie jautājumi

1. Rīgas Tehniskās universitātes (turpmāk – RTU) informācijas sistēmu drošības politika nosaka informācijas sistēmu pārvaldības pamatnostādnes, kas nodrošina RTU informācijas sistēmu drošu lietošanu, ieviešot un uzturot pietiekamu pasākumu kopumu potenciālā vai radītā kaitējuma mazināšanai vai novēršanai.
2. Politika attiecas uz RTU informācijas un komunikācijas sistēmām (turpmāk – Sistēmas) kuras reģistrētas ar RTU rektora rīkojumu apstiprinātā Sistēmu reģistrā, kā arī ar to saistīto informācijas un komunikācijas sistēmu infrastruktūru.

(izteikts 2021. gada 27. decembra Senāta sēdē apstiprinātā redakcijā)

3. Sistēmu drošības pārvaldība tiek organizēta ievērojot samērīguma principu, kur ieviesto drošības pasākumu izmaksas nepārsniedz potenciālā kaitējuma iestāšanās rezultātā nodarītos zaudējumus.

II. Politikā lietotie termini

4. Sistēma - ir iekšējo un ārējo informācijas un tehnisko resursu kopums, kas ir izveidots, strādā un tiek uzturēts, lai vāktu, uzkrātu, apstrādātu, uzglabātu un izmantotu informāciju.
5. Sistēmas lietotājs – fiziska persona, kura lieto Sistēmu saskaņā ar noslēgto līgumu ar RTU.
6. Sistēmu drošības pārvaldnieks (turpmāk – Drošības pārvaldnieks) – persona, kura īsteno Sistēmu drošības pārvaldību RTU.
7. Informācijas resurss – datu faili, datu bāzes, arhīvi u.c. resursi, kurus apstrādā, pārraida, glabā vai veic citas funkcijas neatkarīgi no datu nesēja veida.
8. Tehniskais resurss – datori, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai.
9. Resursa turētājs – tās RTU struktūrvienības vadītājs, kurai Sistēmu reģistrā ir piesaistīta konkrētā Sistēma. Resursa turētājs veic Sistēmu klasifikāciju, drošības risku analīzi, drošības līdzekļu noteikšanu, kā arī nosaka personu loku, kuriem ir atļauta piekļuve Sistēmai.
10. Resursa aizbildnis – persona (kvalificēts tehniskais speciālists), kas veic sistēmas administrēšanas darbus, tajā skaitā atbild par Sistēmas uzturēšanu un tam atbilstošo tehnisko resursu vai kādu to daļu funkcionalitātes nodrošināšanu.
11. Par Sistēmas (-u) drošību atbildīgā persona – ar Senāta lēmumu vai rektora rīkojumu nozīmēta persona RTU struktūrvienībā (-ās).
12. Ielaušanās noteikšanas/novēršanas Sistēma – iekārta vai programmatūra, kas veic Sistēmu aktivitāšu uzraudzību ar mērķi atklāt ļaunprātīgas darbības, tās novērst vai ziņot par tām.
13. Incidents – jebkāda darbība, kuras rezultātā tiek vai var tikt ietekmēta Sistēmu drošība.
14. Integritāte – pilnīgas un nemainītas informācijas saglabāšana.

15. Pieejamība – piekļuve informācijai noteiktā laikposmā pēc informācijas pieprasīšanas.

16. Konfidencialitāte – informācijas nodošana tikai tām personām, kuras ir pilnvarotas to saņemt un lietot.

17. Šifrēšana – veids, kā padarīt datus nelasāmus visiem, izņemot personu, kurai ir atbilstoša šifrēšanas atslēga datu atšifrēšanai.

18. Tehniskie drošības līdzekļi – aizsardzības līdzekļu kopums, kurus izmanto, lai nodrošinātu pietiekamu konfidencialitātes, integritātes un pieejamības līmeni.

III. Sistēmu drošības pārvaldības organizācija un atbildība

19. RTU rektors (turpmāk – rektors) nodrošinot Sistēmu drošību, norīko atbildīgās personas.

20. Rektors ar rīkojumu nosaka Drošības pārvaldnieku – personu, kura organizē un vada RTU Sistēmu drošības pasākumu īstenošanu, ievērojot normatīvajos aktos noteiktās prasības.

21. Nepieciešamības gadījumā, rektors ar rīkojumu atsevišķās struktūrvienībās nosaka par Sistēmas (-u) drošību atbildīgo personu RTU struktūrvienībā.

22. Par Sistēmas drošību atbildīgā persona ir atbildīga par Sistēmu drošības pārvaldību RTU struktūrvienībā un par savas rīcības saskaņošanu ar Drošības pārvaldnieku.

23. Drošības pārvaldnieks izstrādā, aktualizē un ir atbildīgs par Sistēmu klasifikācijas procesu un tā pārraudzību, kā arī Sistēmu reģistra uzturēšanu aktuālā stāvoklī.

24. Drošības pārvaldnieks organizē Sistēmu lietotāju apmācību par Sistēmu drošības jautājumiem.

25. Sistēmu drošības prasības atbilstoši piešķirtajām drošības klasēm nosaka resursa turētājs. Resursa turētājs, saskaņojot ar Drošības pārvaldnieku, ir tiesīgs noteikt piesaistītajai Sistēmai īpašas drošības prasības, ciktāl tās nav pretrunā ar Politiku.

26. Resursa turētājs atbild par sistēmas klasificēšanu, risku analīzi, drošības līdzekļu noteikšanu, kā arī nosaka personas, kurām ir atļauta piekļuve Sistēmai.

27. RTU struktūrvienību vadītājiem ir pienākums sadarboties ar Drošības pārvaldnieku Sistēmu reģistra informācijas uzturēšanā aktuālā stāvoklī, tai skaitā informējot par pārziņā esošām Sistēmām, kuras būtu iekļaujamas Sistēmu reģistrā.

28. Sistēmu integritātes, pieejamības un konfidencialitātes drošības klases pārskata ne retāk kā reizi gadā, kā arī gadījumos, kad izmaiņas ietekmē Sistēmu drošību.

29. Iekšējā audita nodaļa ir atbildīga par Sistēmu auditu organizēšanu un/vai veikšanu un ziņošanu RTU vadībai par konstatēto audita laikā, atklātajiem riskiem, to ietekmi uz RTU, un iesniedz ieteikumus atklāto risku mazināšanai, saskaņā ar Iekšējā audita struktūrvienības nolikumā noteikto.

Sistēmu raksturojums

30. Sistēmas lieto RTU funkciju izpildei nepieciešamās informācijas radīšanai, apkopošanai, uzkrāšanai, apstrādāšanai, lietošanai un iznīcināšanai.

31. Sistēmu fiziskā aizsardzība tiek nodrošināta ņemot vērā to drošības klases.

IV. Sistēmu drošības klases

32. Izvērtējot Sistēmas drošības risku pieņemamo līmeni, resursa turētājs tai piešķir atbilstošo drošības klasi saskaņā ar 2015.gada 28.jūlija Ministru kabineta noteikumu Nr.422 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 7.1.apakšpunktu.

33. Ja Sistēmai piešķirtas trīs B drošības klases vai vismaz viena A drošības klase, Sistēma ir uzskatāma par paaugstinātas drošības Sistēmu. Pārējos gadījumos Sistēma ir uzskatāma par pamata drošības Sistēmu.

V. Sistēmu drošības risku vadība

34. Par Sistēmu drošības risku vadību atbild Resursa turētājs un Drošības pārvaldnieks.

35. Sistēmu drošības risku analīzi veic visām paaugstinātas drošības Sistēmām.

36. Pamata drošības Sistēmām drošības risku analīzi veic, izvērtējot tās nepieciešamību.

37. Sistēmu drošības risku analīzi veic, ja paaugstinātas drošības Sistēmā plāno izdarīt izmaiņas, kas ietekmē Sistēmu drošību.

38. Sistēmu drošības risku analīzi var ierosināt rektors, resursa turētājs, resursa aizbildnis vai Drošības pārvaldnieks.

39. Pirms kārtējās Sistēmu drošības risku analīzes, Drošības pārvaldnieks izvērtē Sistēmu drošības risku pārvaldības plānā noteikto atbildīgo darbinieku ieviestos Sistēmas drošības riskus mazinošos pasākumus.

VI. Sistēmu lietotāji un Sistēmu piekļuves līdzekļi

40. Sistēmu lietotāja tiesību piešķiršanu un anulēšanu, ietverot jaunu lietotāju reģistrāciju un tiesību anulēšanu darba tiesisko vai citu līgumisko attiecību pārtraukšanas gadījumā, veic Sistēmas turētājs vai pārvaldnieks saskaņā ar noteikumiem, kas nosaka lietotāja piekļuves tiesību piešķiršanu un anulēšanu.

41. Sistēmu turētājs vai pārvaldnieks iepazīstina RTU darbiniekus, pirms lietotāja tiesību piešķiršanas, ar RTU iekšējiem normatīvajiem aktiem, kuri nosaka Sistēmu lietotāja tiesības, pienākumus un atbildību.

42. Lietotāju tiesības un pienākumi ir noteikti RTU iekšējos normatīvajos aktos vai, atbilstoši drošības prasībām, noslēgtajos līgumos/vienošanās.

43. Katram Sistēmu lietotājam tiek piešķirts individuāls identifikators un parole (vismaz 9 simboli), kas, pirmo reizi reģistrējoties Sistēmās, obligāti ir jānomaina.

44. Katrs lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja Sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētajai fiziskajai personai, tad Sistēmā ir iestrādāti tehniskie līdzekļi, kas novērš iespēju lietotājiem izmantot šos kontus.

45. Sistēmu lietotājam ir piekļuve tikai tiem informācijas un tehniskajiem resursiem, kuri tam ir nepieciešami darba pienākumu veikšanai (Sistēmu funkcijas izpildāmas ar minimāli iespējamām tiesībām).

46. Sistēmu lietotājiem, kuriem pieejas tiesību pamatojums ir darba tiesiskās attiecības ar RTU, lietotāja tiesības tiek anulētas ar dienu, kad starp RTU un Sistēmas lietotāju tiek izbeigti visi darba tiesisko attiecību līgumi. Resursa turētājam ir tiesības noteikt īpašus izņēmuma gadījumus.

47. Atkarībā no veicamajiem pienākumiem, Sistēmu lietotāji izmanto īpašus lietotāju kontus, kuri tiem tiek piešķirti.

48. Ir aizliegts elektroniski glabāt un transportēt nešifrētā veidā datus, Sistēmas lietotāja paroles, tajā skaitā iegūtos Sistēmas lietotāja autentifikācijas procesa ietvaros.

49. Ne retāk kā vienu reizi gadā resursa turētājs pārskata savā pārziņā esošās Sistēmas lietotāju piekļuves tiesības.

50. Trešo pušu (piegādātāji, konsultanti u.c.) piekļuve Sistēmai (izņemot publiskos informācijas resursus) tiek īstenota saskaņā ar līgumattiecībām un RTU iekšējiem normatīvajiem aktiem.

51. Drošības pārvaldnieks par Sistēmu lietošanas noteikumu neievērošanu Sistēmas lietotājam ir tiesīgs anulēt lietotāja piekļuves tiesības.

52. Drošības pārvaldnieks, brīdinot atbildīgo personu (resursa aizbildni) par IP adresi (sistēmu), vai, ja tādu nevar noskaidrot, RTU Lietotāju atbalsta centru, ir tiesīgs atslēgt informācijas sistēmu vai ierīci no tīkla, gadījumos, kad ir pamatotas aizdomas, ka tā tiek vai var tikt izmantota ļaunprātīgu darbību veikšanai. Informācijas sistēma vai ierīce tiek pieslēgta tīklam pēc tam, kad atbildīgā persona (resursa aizbildnis) ir veicis atbilstošas darbības, lai novērstu ierīces ļaunprātīgu izmantošanu.

(pievienots pamatojoties uz 2021. gada 27. decembra Senāta lēmumu)

VII. Sistēmu izstrāde un uzturēšana

53. Sistēmu drošības prasības tiek identificētas un dokumentētas katrā ar Sistēmas izstrādi saistītā projekta prasību noteikšanas fāzē, veicot to pamatošanu un saskaņošanu ar resursa turētāju.

54. Ekspluatācijas Sistēmas nodala no izstrādes un testa Sistēmām, attiecīgi tās apzīmējot, un lieto no ekspluatācijas Sistēmas atšķirīgus lietotāja identifikatorus un paroles vai, lietojot vienādus lietotāja identifikatorus un paroles, nodrošina līdzvērtīgas drošības prasības testa un ekspluatācijas Sistēmai.

55. Par Sistēmas reģistrēšanu Sistēmu reģistrā atbild RTU struktūrvienības vadītājs, kurš ir pasūtījis Sistēmas izstrādi.

56. Pasūtot Sistēmas izstrādi, tiek noteikts, ka:

56.1. ir pieejams Sistēmas datorprogrammu pirmkods un tā lietošanas tiesības tiek nodotas RTU;

56.2. ir noteikts Sistēmas uzturēšanas un atbalsta nodrošināšanas (tai skaitā Sistēmas drošības nepilnību novēršanas) laikposms;

56.3. pirms jaunas Sistēmas pieņemšanas ekspluatācijā tai ir veikti ielaušanās testi.

57. Piekļuve Sistēmas failiem (t.sk. programmatūras pirmkodam) tiek kontrolēta, nodrošinot izmaiņu vadību un piekļuves mēģinājumu auditāciju.

58. Sistēmā tiek iestrādāti drošības līdzekļi, korektai datu ievadei un apstrādei.

59. Sistēmā, kas nodrošina elektroniskā pasta saņemšanu no ārējiem resursiem, ienākošo saziņu apstrādā vismaz atbilstoši e-pastu autentifikācijas protokola (DMARC) prasībām, ieviešot e-pasta apstrādi atbilstoši sūtītāja domēna vārda DMARC politikai, atskaites ģenerēšanu un nosūtīšanu DMARC konfigurācijā norādītajam kontaktam
(pievienots pamatojoties uz 2021. gada 27. decembra Senāta lēmumu)

60. Iekārtām, tajā skaitā infrastruktūras iekārtām, kas nodrošina Sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles.

61. RTU tiek īstenota programmatūras ievainojamību regulāra uzraudzība, nodrošinot operatīvu programmatūras labojumu instalāciju gan operētājsistēmām, gan citai lietotajai programmatūrai.

VIII. Sistēmu drošības incidentu vadība

62. RTU tiek uzturēts Sistēmu drošības incidentu uzskaites žurnāls.

63. Resursu aizbildņi atklāj un reģistrē Sistēmu drošības incidentus Sistēmu drošības incidentu uzskaites žurnālā.

64. Sistēmas drošības incidenta atklāšanas gadījumā tiek informēts Drošības pārvaldnieks, kurš pieņem lēmumu par turpmākām darbībām incidenta novēršanai.

65. Visās RTU esošajām galalietotāju iekārtās, kas tiek izmantotas, lai pieslēgtos Sistēmai, ir jābūt iekļautai pretvīrusu funkcionalitātei.

66. RTU lieto automatizētās ielaušanās noteikšanas/novēršanas Sistēmu.

67. RTU tiek nodrošināta Sistēmas auditācijas pierakstu veidošana un uzglabāšana vismaz 6 (sešus) mēnešus pēc ieraksta izdarīšanas. Paaugstinātas drošības Sistēmām – 18 (astoņpadsmit) mēnešus pēc ieraksta izdarīšanas.

68. Jebkura piekļuve Sistēmām ir izsekojama līdz konkrētam Sistēmas lietotāja kontam vai interneta protokola (IP) adresei.

IX. Sistēmu nepārtrauktās darbības vadība

69. Drošības pārvaldnieks izstrādā un vada Sistēmu nepārtrauktās darbības plānu, paredzot, ka darbības Sistēmu nepārtrauktības nodrošināšanas izmaksām ir jābūt samērojamām ar iespējamiem zaudējumiem, kas varētu rasties no Sistēmas darbības pārtraukuma.

70. Darbības nepārtrauktības pasākumi tiek koncentrēti uz RTU pamatdarbības procesu un paaugstinātas drošības Sistēmām, nosakot pasākumus, kas nodrošina procesu un pakalpojumu atjaunošanu pēc nozīmīga Sistēmas incidenta.

71. Ar darbības nepārtrauktību saistītie dokumenti tiek aktualizēti, testēti un pārskatīti pēc izmaiņu veikšanas Sistēmā, vai vismaz reizi gadā.

X. Noslēguma jautājums

72. Kārtību, kādā RTU tiek organizēta droša Sistēmu lietošana, nosaka rektora apstiprināti iekšējie normatīvie akti.