LATVIJAS REPUBLIKAS IZGLĪTĪBAS UN ZINĀTNES MINISTRIJA
RĪGAS CELTNIECĪBAS KOLEDŽA
Reģ. Nr. 3347001284
Gaiziņa iela 3, Rīga, LV-1050; tālrunis: (+371) 67229714; e-pasts: sekretare@rck.lv

Iekšējie noteikumi Nr. 01-45/4

Rīgā 18.02.2021.

Rīgas Celtniecības koledžas Informācijas tehnoloģiju drošības noteikumi

Izdoti pamatojoties uz 08.05.2007. Ministru kabineta noteikumu Nr.297 "Rīgas Celtniecības koledžas nolikums" 53.punktu

I. Vispārīgie jautājumi

1. Rīgas Celtniecības koledžas (turpmāk – RCK) Informācijas tehnoloģiju (turpmāk – IT) drošības noteikumi (turpmāk – noteikumi) izstrādāti saskaņā ar Informācijas tehnoloģiju drošības likumu.
2. Noteikumi nosaka kārtību, kādā RCK nodrošina tai piederošo informācijas un tehnisko resursu (turpmāk – resursi) aizsardzību.
3. Noteikumi ietver minimālās prasības. Informācijas sistēmas resursu turētājs var noteikt stingrākus drošības pasākumus.
4. Noteikumu mērķis ir:
4.1. apliecināt RCK vadības apņemšanos nodrošināt resursu drošību, lai uzturētu to integritāti, pieejamību un konfidencialitāti;
4.2. nodrošināt vienādu un sistemātisku pieeju informācijas tehnoloģiju drošības jautājumu risināšanai visā RCK;
4.3. panākt RCK darbinieku izpratni par informācijas tehnoloģiju drošības jautājumiem;
4.4. būt par pamatu procedūru, instrukciju un citu nepieciešamo drošības dokumentu izstrādē un ieviešanā.
5. Noteikumu ievērošana ir obligāta visiem RCK IT resursu lietotājiem.

II. Noteikumos lietotie termini

6. Informācijas resursi – dažādu informācijas sistēmu sistēmprogrammas, sistēmu un datu faili un cita informācija, ko izmanto informācijas apstrādei, pārraidei, glabāšanai un citu funkciju veikšanai.
7. Tehniskie resursi – serveri, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai.

8. Resursu turētājs – RCK direktors vai ar RCK rīkojumu iecelts darbinieks, kurš ir atbildīgs par IT drošības pārvaldību.
9. Resursu lietotājs – RCK darbinieks, uz uzņēmuma līguma pamata nodarbinātais vai studējošais, kurš izpilda noteiktus pienākumus un apstrādā noteiktu informāciju atbilstoši piešķirtām tiesībām lietot noteiktus informācijas resursus.
10. Informācijas integritāte – raksturo, cik lielā mērā informācija ir pilnīga, patiesa, precīza un aktuāla.
11. Informācijas pieejamība – raksturo, vai lietotāji var piekļūt nepieciešamajai informācijai ne vēlāk kā noteiktā laikā pēc informācijas pieprasīšanas brīža.
12. Informācijas konfidencialitāte – raksturo, cik lielā mērā informācija ir pieejama tikai šīs informācijas saņemšanai paredzētajiem lietotājiem.
13. Informācijas vērtība – informācijas nozīmīgums iestādes funkciju veikšanai.
14. Drošības incidents – kaitīgs notikums vai nodarījums, kas apdraud informācijas resursu integritāti, pieejamību vai konfidencialitāti.
15. Auditācijas pieraksti – analīzei pieejams resursu veikto darbību (piekļūšana, datu ievade, mainīšana, dzēšana, izvade) atspoguļojums elektroniskas informācijas veidā.
16. Drošības dokumenti – dokumentu kopums, kas apraksta iestādes resursu lietošanas kārtību.
17. Risku pārvaldīšana – informācijas sistēmu risku identificēšana, novērtēšana, samazināšana un kontrolēšana, kuras ietvaros tiek veikta informācijas sistēmu risku ierobežošana līdz iestādei pieņemamam līmenim.
18. Ārpakalpojuma sniedzējs – trešā persona, kas uz līguma pamata nodrošina iestādes IT drošības pārvaldību vai citas funkcijas.

III. Fiziskā resursu aizsardzība

19. RCK datortīklu administrators risku pārvaldības ietvaros veic IT fiziskās aizsardzības pasākumus, kas aizsargā tās no nevēlamiem apkārtējās vides faktoriem (ugunsgrēks, plūdi, temperatūras svārstības u.c.), tehniskajiem faktoriem (neatbilstoša elektroenerģijas piegāde u.c.) un cilvēkfaktoriem (tīši vai netīši bojājumi, zādzība u.c.).

IV. Tīklu infrastruktūra

20. RCK datortīklu administrators nodrošina pietiekamu fizisko aizsardzību tīkla aparatūrai un kabeļiem, tos izvietojot tādējādi, lai tiem nevarētu nesankcionēti, nemanīti vai aiz nejaušības piekļūt, pieslēgties vai kā citādi bojāt.

V. Darbstaciju fiziskā aizsardzība

21. Darbstacijas lieto atbilstoši ražotāja noteiktajām prasībām.
22. Lietot elektroenerģijas nepārtrauktas piegādes iekārtas, ja elektroenerģijas piegādes traucējumu radītais risks ir nepieņemami liels.

VI. Portatīvo iekārtu fiziskā aizsardzība

23. Portatīvos datorus lieto atbilstoši ražotāja noteiktajām prasībām.
24. RCK datortīklu administrators veic portatīvo iekārtu aprites reģistrēšanu, lai noteiktu, kura persona lieto attiecīgo iekārtu.

VII. Datu nesēju fiziskā aizsardzība

25. Datu nesējus, kas satur informācijas resursus, lietot un pārvietot bez īpaša laika ierobežojuma drīkst tikai RCK resursu turētāja pilnvaroti darbinieki, kuriem ir pieeja informācijas resursiem. Informācijas resursi, kurus nav nepieciešams lietot vai pārvietot, tiek glabāti RCK telpās tam paredzētās vietās.
26. Resursu lietotājiem datu nesējus ar klasificētiem informācijas resursiem aizliegts atstāt nedrošās, publiski pieejamās vietās.

VIII. Piekļuves kontrole

27. Katram resursu lietotājam tiek piešķirts lietotāja vārds un parole, kā arī noteiktas piekļuves tiesības. Lietotājs ir atbildīgs par piešķirtās paroles lietošanu, saglabāšanu un neizpaušanu.
28. Resursu turētājs apstiprina piekļuves tiesības. Balstoties uz resursu turētāja norādījumu, resursu administrators izveido piekļuvi lietotājam visās norādījumā uzskaitītajās informācijas sistēmās.
29. Resursu turētajam vai tā pilnvarotai personai ir jāinformē datortīklu administratoru par tiem darbiniekiem un studējošajiem, kuri pārtrauc darba vai studiju attiecības ar RCK. Datortīklu administrators pēc šīs informācijas saņemšanas nekavējoties anulē visas attiecīgā lietotāja piekļuves tiesības RCK informācijas sistēmas resursiem.
30. Lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotāja vārdu. Lietotāja autentiskumu nosaka, lai pārliecinātos, ka lietotāja vārda izmantotājs ir sankcionētais tā turētājs. Autentiskuma noteikšanai tiek izmantotas paroles. Pēc lietotāja vārda un paroles ievadīšanas lietotājs var izmantot informācijas resursu atbilstoši noteiktajām piekļuves tiesībām.
31. Par paroli nedrīkst izmantot personu identificējošus datus (piemēram, personas datus, automašīnas numuru, radu vārdus vai uzvārdus, vārdus, kas saistīti ar darbavietu vai kas bieži tiek tajā lietoti).
32. Lietotāji paši ir atbildīgi par savu paroļu drošu glabāšanu.
33. Lietotājam pirmo reizi autorizējoties sistēmās, parole ir jānomaina.
34. Paroles uzbūvei jābūt komplicētai, izmantojot burtu, ciparu un īpašo rakstzīmju kombināciju (piemēram, !@#$%^*()_+). Paroles garumam resursiem, ir jābūt vismaz 8 (astoņiem) simboliem.
35. Lietotājam regulāri, ne retāk kā 1 (vienu) reizi 3 (trīs) mēnešos jāmaina lietošanas parole.
36. Lietotāju paroles uz serveriem var glabāt tikai šifrētā veidā.
37. Lietotājam parole ir jāiegaumē. Rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā seifā ar ierobežotu pieeju vai izmantot speciāli šim nolūkam paredzētus rīkus.
38. Lietotājam ir aizliegts izpaust jebkuru piešķirto paroli, kā arī citu konfidenciālu informāciju, kas saistīta ar IT resursu izmantošanu. Par katru darbību, kas veikta datoru tīklā, datu bāzēs, kā arī citās informatīvās sistēmās, ir atbildīgs izmantotā lietotāja vārda un paroles īpašnieks.
39. Izmantojot RCK IT resursus publiskās vietās, lietotajam ir jāpārliecinās, ka, beidzot darbu, sistēma ir pieejama tikai no jauna autentificējoties – lietotājam ievadot lietotāja vārdu un paroli.
40. Ja lietotājs konstatē, ka kāds cits ir uzzinājis viņa paroli, lietotājs to nekavējoties nomaina un par to nekavējoties ziņo datortīklu administratoram.

41. Aizliegts mēģināt uzzināt citu lietotāju paroles.
42. Datortīklu administratoram, instalējot sistēmu, jānomaina noklusētās paroles.

IX. Datu rezerves kopiju veidošana

43. RCK datortīklu administrators regulāri veic svarīgāko koplietošanas informācijas resursu un programmatūru rezerves datu kopēšanu. Rezerves datu kopēšanu nodrošina resursu administrators, un to biežums un apjoms tiek saskaņots ar resursu turētāju.
44. Vismaz reizi dienā tiek veidota inkrementālā dublējumkopija resursu datnēm. Resursu administrators pārbauda, ka rezerves kopiju veidošanas process ir beidzies sekmīgi.
45. Nodzēstu datu atjaunošana tiek nodrošināta vismaz 30 (trīsdesmit) dienas.
46. Reizi gadā resursa administrators pārbauda iespēju no rezerves kopijām atjaunot informācijas resursu datus.
47. Rezerves datu kopijas tiek glabātas tikai šim mērķim paredzētā datu nesējā.

X. Resursu loģiskā aizsardzība

Risku pārvaldības ietvaros
48. RCK risku pārvaldības ietvaros:
48.1. datortīklu administrators veic informācijas resursu loģiskās aizsardzības pasākumus, dokumentē resursus un veic resursu lietotāju reģistrācijas, tiesību piešķiršanas un anulēšanas procedūras;
48.2. katram lietotājam piešķir unikālu lietotāja vārdu pieejai informācijas resursiem. Jauna lietotāja reģistrāciju veic saskaņā ar IT drošības politiku un RCK IT drošības noteikumiem. Resursu lietotāju darba pienākumu vai studiju maiņas vai darba attiecību izbeigšanas gadījumā tiek nekavējoties mainīti vai anulēti piešķirtie lietotāja vārdi un pieejas tiesības informācijas resursiem;
48.3. datortīklu administratora pieejas vārdus kopā ar parolēm rakstiskā veidā var glabāt tikai aizslēgtā seifā ar ierobežotu pieeju vai izmantot speciāli šim nolūkam paredzētus rīkus;
48.4. datortīklu administrators atbilstoši resursu turētāja norādījumiem periodiski (vismaz reizi gadā) pārskata (auditē) lietotāju tiesības, lai nodrošinātu nevajadzīgu kontu anulēšanu vai tiesību maiņu, lai tikai autorizētiem lietotājiem ir piekļuve informācijas resursiem un lietotājiem ir piešķirtas tikai tās tiesības, kas nepieciešamas darba pienākumu pildīšanai.

Lietotāju autentiskuma noteikšanas ietvaros
49.Lietotāju autentiskuma noteikšanas ietvaros:
49.1.resursu administrators pārliecinās, ka attiecīgos informācijas resursus lieto pilnvarotais lietotāja vārda turētājs, izmantojot dažādus pietiekamas drošības autentifikācijas līdzekļus, kas var tikt pilnveidoti, mainīti un attīstīti;
49.2. autentifikācijas līdzekļu lietošanas veidus un kārtību nosaka RCK IT drošības politika, bet tehniski nodrošina datortīklu administrators;
49.3. resursu lietotājam un administratoram par paroli jāizvēlas pietiekami sarežģīta simbolu kombinācija. Ievadot paroli, tā nedrīkst būt salasāma uz datora ekrāna. Paroles elektroniskajos nesējos glabā un pārsūta šifrētas. Paroli nekavējoties nomaina, ja tā varētu būt vai ir kļuvusi zināma citai personai.

XI. Vīrusu kontrole

50. Vīrusu kontrole informācijas resursos:
50.1. datortīklu administrators nosaka kārtību un veic pasākumus datorvīrusu darbības novēršanai informācijas sistēmās;
50.2. vīrusu darbības novēršanai lieto speciāli šim nolūkam paredzētu programmatūru. Vīrusu definīciju failus nekavējoties atjauno, tiklīdz izstrādātājs tos piedāvā;
50.3. resursu administrators regulāri veic antivīrusu programmas pārraudzību, lai pārliecinātos par tās darbību un jaunāko vīrusu definīciju failu esamību.

XII. Darbstaciju aizsardzība

51. Personālo un portatīvo datoru aizsardzība:
51.1. portatīvajos datoros, kuri tiek lietoti ārpus RCK darba telpām, glabā tikai to informāciju, kas nepieciešama noteiktajā laikā noteiktajam datora lietotājam;
51.2. personālajā datorā uzstāda un lieto tikai to programmatūru un tādā konfigurācijā, ko ir noteicis resursu turētājs. Resursu administrators personālā datora funkcionalitāti ierobežo līdz darba vajadzībām nepieciešamo funkciju līmenim;
51.3. lietotājam atstājot personālo datoru bez uzraudzības, to slēdz, lietojot ekrānsaudzētāju ar paroli, speciālu slēgšanas funkciju vai citu metodi, kas ļauj turpināt darbu ar personālo datoru vienīgi tad, ja ir veikta lietotāja autentifikācija.

XIII. Datortīklu aizsardzība

52. Datortīklu aizsardzība:
52.1. datortīklu administrators izstrādā un uztur datortīkla shēmu, kurā parādīta datortīklā savienotā aparatūra un nodrošinātie pakalpojumi;
52.2. datu plūsmā starp lokālo datortīklu un ārējo datortīklu atļauj tikai tos pakalpojumus, kas ir nepieciešami RCK funkciju izpildei, šim nolūkam lietojot ugunsmūra sistēmu;
52.3. resursu administrators pārbauda visu ārējo savienojumu eksistenci un pārliecinās, ka pastāv tikai tie savienojumi, kuri atbilst RCK darbības vajadzībām, un ka darbojas rezerves savienojumi;
52.4.pieslēgšanos RCK informācijas sistēmām no loģiski attālas vietas aizsargā, lietojot kriptogrāfijas līdzekļus kopā ar lietotāja vārdu tā, lai droši noteiktu lietotāja autentiskumu.
53. Datortīklu administratoram pēc nepieciešamības iesaka papildu loģiskās aizsardzības pasākumus atkarībā no informācijas resursu klasifikācijas.

XIV. RCK sadarbība ar ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem

54. Ja RCK izvēlas resursa uzturēšanu uzticēt ārējam pakalpojumu sniedzējam, tam jānodrošina drošības līmenis, kas nav zemāks par šajos noteikumos noteikto.
55. RCK nosaka informācijas izpaušanas ierobežojumus.
56. Ārpakalpojuma līgumā jāiekļauj Informācijas tehnoloģiju drošības likumā noteiktie pienākumi.
57. Saskaņojot ar resursu turētājiem, piešķir pieejas tiesības informācijas resursiem ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem tikai to pienākumu veikšanai nepieciešamajā apjomā.
58. Visas izmaiņas (sistēmas informācijas resursu izveidošana, papildināšana,

mainīšana, apstrāde, pārraidīšana, glabāšana, atjaunošana un iznīcināšana) notiek atbilstoši RCK IT izmaiņu pārvaldības prasībām.

Direktors  N.Grinbergs

Sagatavoja U.Timpers