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. 01-45/5

Rīgā 18.02.2021.

RCK Informācijas tehnoloģiju drošības politika

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

I. Vispārīgie jautājumi

1. Lai noteiktu organizācijas informācijas sistēmu drošības principus, ir noteikta kopēja Rīgas Celtniecības koledžas (turpmāk – RCK) informācijas tehnoloģiju (turpmāk – IT) drošības politika, kas aptver esošās informācijas sistēmas, nosakot atbildīgos IT drošības jomā, un pauž RCK vadības nostāju, kāpēc organizācijas rīcībā esošā informācija ir svarīga tās mērķu īstenošanai un kā tiek nodrošināta informācijas un tehnisko resursu aizsardzība.
2. IT drošības politikas uzdevums ir definēt RCK vadības nostāju un atbalstu informācijas drošības nodrošināšanai atbilstoši RCK vajadzībām, spēkā esošajiem normatīvajiem aktiem un drošības normām.
3. IT drošības politikas nostādnes tiek noteiktas atbilstoši RCK mērķiem un stratēģijai.
4. IT drošības politika ieņem centrālo vietu RCK IT drošības organizēšanā, un no tās izriet visi ar IT drošību saistītie noteikumi, kārtības, procedūras, plāni un rīkojumi. IT drošības politikas nostādnes ir jāzina ikvienam RCK darbiniekam.

II. IT drošības politikas pamatnostādnes

5. RCK IT drošības politika (turpmāk – drošības politika) ir izstrādāta un tiek īstenota saskaņā ar RCK darbības mērķiem un uzdevumiem, Latvijas Republikā spēkā esošajiem normatīvajiem aktiem, kā arī ņemot vērā starptautisko IT drošības standartu rekomendācijas.
6. Drošības politika ir izstrādāta ar mērķi nodrošināt tādu IT vidi, lai RCK informācijas un tehniskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības riskiem un vienlaikus nodrošinātu RCK nepārtrauktu un kvalitatīvu darbību atbilstoši normatīvajos

aktos noteiktajām funkcijām.
7. Drošības politika nosaka galvenos drošības pamatnosacījumus IT videi un kārtību informācijas un tehnoloģisko resursu aizsardzības nodrošināšanai RCK.
8. Drošības politika ir saistoša visiem RCK darbiniekiem, kā arī tiem ārpakalpojumu sniedzējiem, kuri RCK sniedz ar IT saistītus pakalpojumus vai izmanto RCK informācijas sistēmas.

III. Drošības politikas īstenošanas pamatprincipi

9. RCK ir noteikts un pastāvīgi tiek pilnveidots dokumentu un pasākumu kopums, kura īstenošana nodrošina drošības politikas mērķu sasniegšanu.
10. Risku ierobežošanas un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties šo risku īstenošanās vai RCK darbības pārtraukšanas gadījumos.
11. RCK tiek sekmēta katra darbinieka izpratne par pienākumiem risku un darbības nepārtrauktības pārvaldīšanā un informācijas un tehnoloģisko resursu aizsardzības nodrošināšanā, veicot RCK darbinieku regulāru izglītošanu.
12. RCK tiek nodrošināta pastāvīga drošības politikas īstenošanas koordinēšana un pārraudzīšana.
13. Gadījumos, kad RCK darbinieki neievēro IT drošības politikas izvirzītās prasības, RCK vadība var ierosināt disciplinārās sodīšanas procesu saskaņā ar spēkā esošajiem normatīvajiem aktiem.

IV. Drošības organizēšana

14. Resursu turētājs. RCK vadība kopumā ir atbildīga par informācijas drošības politikas īstenošanu, t.sk. par IT drošības organizēšanas izveidi un atbildības noteikšanu, kontroles noteikšanu un adekvātu resursu piešķiršanu IT drošības organizēšanas pilnvērtīgai funkcionēšanai.
15. Informācijas lietotājs. Informācijas lietotājs ir atbildīgs par visām darbībām, kuras ir veiktas ar viņa lietotāja vārdu. Lietotāja pienākums ir informēt resursu administratoru un/vai RCK datortīklu administratoru par IT drošības incidentiem un aizdomīgiem notikumiem.

V. Resursu piederība

18. Visi informācijas un tehnoloģiskie resursi pieder RCK.

Direktors N.Grinbergs

Sagatavoja U.Timpers