APSTIPRINĀTI

2018. gada ___. maijā

Rektora v.i. _____

Videonovērošanas sistēmas datu aizsardzības noteikumi

I Vispārējie noteikumi

1. AS "TRANSPORTA UN SAKARU INSTITŪTS" (turpmāk – Augstskola), Reģ. Nr. 40003458903, Lomonosova 1, Rīga, LV-1019 videonovērošanas sistēmas datu aizsardzības noteikumi (turpmāk – Noteikumi) nosaka videonovērošanas rezultātā iegūto datu apstrādi, lietošanu un aizsardzību, kā arī videonovērošanas tehnikas uzstādīšanas kārtību.

2. Noteikumi izstrādāti atbilstoši Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula) un citām Latvijas Republikas tiesību aktos noteiktajam prasībām, kas attiecas uz videonovērošanas sistēmu lietošanu, izmantošanu un drošību.

3. Videonovērošanas sistēmas mērķis ir aizsargāt Augstskolas īpašumu, gādāt par darbinieku un studējošo drošību, novērst iespējamos likumpārkāpumus, fiksēt noziedzīga nodarījuma izdarīšanas faktu, kā arī identificēt iespējamo likumpārkāpēju (nodrošinot pierādījumu tiesiskumu), potenciāli bīstamu priekšmetu atklāšanā un pārbaudē, un potenciālo lietu atrašanā.

4. Noteikumi ir saistoši visiem videonovērošanas sistēmas personas datu apstrādes lietotājiem (personām, kurām piešķirtas sistēmas lietotāja tiesības). Noteikumi ir attiecināmi uz visiem personas datiem, kas tiek ierakstīti videonovērošanas kamerās (videonovērošanas ierakstā).

5. Videonovērošana un tās rezultātā iegūto personas datu apstrāde tiek veikta Augstskolas iekšējās telpās, uz ko norāda īpaša zīme, ko novieto pie ieejas videonovērošanas zonā saskaņā ar paraugu. Zīme satur informāciju par sistēmas Pārzini un tā kontaktinformāciju.

VIDEONOVĒROŠANA
Mērķis: Noziedzīgu nodarījumu novēršana un atklāšana saistībā ar īpašuma aizsardzību
Pārzinis: AS "TRANSPORTA UN SAKARU INSTITŪTS", Reģ. Nr. 40003458903
Juridiskā adrese: Lomonosova 1, Rīga, LV-1019

6. Par videonovērošanas rezultātā iegūtu personas datu apstrādes aizsardzības drošību Augstskolā atbild par drošību atbildīgā persona – Datoru tehnoloģiju daļas vadītājs (turpmāk – Lietotājs).

II Informācijas klasifikācija un lietotāja tiesību piešķiršana

7. Dati, kas tiek ierakstīti ar videonovērošanas kameru palīdzību, ir kvalificējami kā ierobežotas piekļuves informācija, jo satur personu identificējošos datus. Tiesības piekļūt un veikt šo datu apstrādi ir tikai pilnvarotajām identificētiem sistēmas lietotājiem.

8. Lietotāju, kuram atļauts veikt personas datu apstrādi, piekļūšanu videonovērošanas programmatūrai un tās veiktajiem ierakstiem, nozīmē par drošību atbildīgā persona – Valdes priekšsēdētāja.

III Lietotāja pienākumi, tiesības un atbildība

9. Lietotāja tiešie pienākumi, tiesības un atbildība ir ietverti katra lietotāja amata (darba) aprakstā.

10. Lietotāja pienākums ir iepazīties ar Noteikumiem pret parakstu un ievērot tos ikdienas darbā. Lietotājs apņemas saglabāt un nelikumīgi neizpaust personas datus.

11. Lietotājam ir tiesības:

11.1. Izmantot lietošanā nodoto tehniku, lai organizētu videonovērošanas attēla ierakstīšanu;

11.2. Pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi vai arī lietotājam ir pietiekams pamats uzskatīt, ka ir iespējami draudi (apdraudējums);

11.3. Atļaut piekļūt videonovērošanas rezultātā iegūtajiem personas datiem attiecīgajam datu subjektam (tikai par sevi): citām personām, ja tas nepieciešams to darba pienākumu izpildei, atbilstoši Noteikumu 8.punktā noteiktajam pilnvarojumam un vienīgi saskaņā ar Noteikumu 3.punktā noteikto datu apstrādes mērķi.

12. Lietotājam aizliegts:

12.1. Izpaust ziņas par Augstskolas videonovērošanas sistēmas tīkla uzbūvi un konfigurāciju, kā arī atklāt klasificēto informāciju nepiederošām personām;

12.2. Atļaut piekļūt videonovērošanas rezultātā iegūtajiem personas datiem (videonovērošanas ierakstiem) citām personām, ja tas nav saistīts ar tiešo darba pienākumu pildīšanu un ja šādu pilnvarojumu nav devusi Augstskolas valde (8.punkts);

12.3. Kopēt personu datus saturošos failus uz ārējiem datu nesējiem (disketēm, USB kartēm un/vai kompaktdiskiem), ja tas nav saistīts ar tiešo darba pienākumu pildīšanu un ja šādu pilnvarojumu nav devusi Augstskolas valde (8.punkts).

13. Lietotājs ir atbildīgs:

13.1. Par videonovērošanas tehniku, kas nodota viņa rīcībā;

13.2. Par darbībām, kas tiek veiktas ar viņam nodoto videonovērošanas tehniku;

13.3. Par datu saglabāšanu, nepieļaujot to nelikumīgu apstrādi, personas datu nejaušu zaudēšanu, iznīcināšanu vai sabojāšanu un prettiesisku nodošanu.

14. Videonovērošanas sistēmas uzturēšanas personālam ir pienākums vienu reizi trijos mēnešos nodrošināt videonovērošanas tehnikas pieejas kodu (kas sastāv no 8 simboliem) nomaiņu. Gadījumā, ja citai personai kļuvis zināms pieejas kods, tas jānomaina nekavējoties, lai tiktu nodrošināti attiecīgi drošības pasākumi.

15. Lietotājs apņemas saglabāt informācijas konfidencialitāti arī pēc darba tiesisko attiecību izbeigšanos.

16. Augstskolas Valde ir tiesīga izpaust videonovērošanas rezultātā iegūtos personas datus tikai tiesībaizsardzības iestādēm likumā noteiktajā kartībā saskaņā ar viņu pieprasījumu. Gadījumos, kad ir nepieciešama personas datu izpaušana, jānodrošina pierakstu esamība par to, kam (identificējot personu), kad, kādam mērķim un kādi personas dati ir izpausti. Gadījumā, ja uz tiesiska pamata ir izdoti

videonovērošanas dati citai personai, par tālāku personas datu apstrādi un likumību atbild persona, kura datus saņēmusi.

17. Augstskola veic uzskaiti par personām, kuras tiek iesaistītas videonovērošanas sistēmas personas datu apstrādē.

IV Videonovērošanas tehnikas uzstādīšana, programmas lietošana un informācijas saglabāšana

18. Videonovērošanas tehnikas un tas programmatūras uzstādīšanu un administrēšanu nodrošina Augstskolas noteiktajā kārtībā par drošību atbildīgais – Lietotājs (Datoru tehnoloģiju daļas vadītājs).

19. Uzstādot videonovērošanas kameras, jāizvēlas tāds kameru izvietojums, lai tas būtu drošībā no neatļautas piekļuves un aizsargātu tās no bojājumiem.

20. Videonovērošanas rezultātā iegūto personas datu apstrādes serveriem ir jābūt novietotiem atsevišķā telpā vai slēdzamā serveru statnē ar ierobežotu pieeju, lai nodrošinātu drošību no neatļautas piekļuves un aizsargātu to no fiziskiem bojājumiem.

21. Veicot videonovērošanu tiek ievēroti šādi nosacījumi:

21.1. Ierakstītajiem vai izdrukātajiem attēliem, tāpat ka attēliem tiešraidē monitorā ir jābūt atbilstošā kvalitātē. Ir jānodrošina, ka nenotiek nevēlami attēla detaļu izkropļojumi ierakstīšanas procesā.

21.2. Digitālajās ierakstu sistēmās ir jāizvēlas atbilstošs datu saspiešanas (kompresijas) lielums, lai neietekmētu attēla kvalitāti;

21.3. Uz ierakstu attēliem jābūt precīzam laikam un datumam, kad ieraksts tiek vai ir veikts;

21.4. Jānodrošina pastāvīga videonovērošanas kameru tehniskā apkalpošana, lai nodrošinātu, ka videonovērošanas kameras turpina veikt nepieciešamajam mērķim attiecīgas kvalitātes ierakstus;

21.5. Ja tiek lietota bezvadu datu pārraide, jānodrošina attiecīgi drošības pasākumi, lai datu pārraidē nebūtu pārrāvumu, kā arī dati netiktu pārtverti.

22. Lietotājam ir aizliegts jebkādā veidā mainīt lietošanā saņemtās videonovērošanas tehnikas un programmatūras konfigurāciju, kā arī instalēt programmatūru.

23. Augstskola ir atbildīga par videonovērošanas tehnikas tehnisko stāvokli, nodrošinot ierakstu kvalitāti un nepieļaujot nevēlamus attēlu/datu detaļu izkropļojumus ierakstīšanas procesā vai uzglabāšanas laikā.

24. Videonovērošanas rezultātā iegūtās informācijas glabāšanas ilgums tiek noteikts – 31 dienas. Pēc šī termiņa beigām Augstskola nodrošina pilnīgu datu dzēšanu, ja dati iepriekš nav pieprasīti vai nav konstatēti noziedzīgi nodarījumi. Ja dati iepriekš ir pieprasīti no kompetentām valsts vai pašvaldību iestādēm vai ir konstatēti noziedzīgi nodarījumi, datus uzglabā pēc nepieciešamības.

25. Videonovērošanas attēlu pārraide (novērošana tiešsaistē) un ierakstu aplūkošana ir jānodrošina atsevišķā telpā vai tādā veidā, lai nepiederošām personām nebūtu iespēja redzēt attēlu monitorus.

26. Videonovērošanas kameras nedrīkst izmantot, lai ierakstītu sarunas starp cilvēkiem. Videonovērošanai tiek izvēlētas iekārtas bez audioieraksta funkcionalitātes vai arī tā tiek atslēgta.

27. Par katru nelikumīgu piekļuvi videonovērošanas tehnikai (kamerām) un/vai ierakstu datiem nekavējoties jāziņo šo Noteikumu 18.punktā minētajai atbildīgajai personai, kas attiecīgi dokumentē nelikumīgās piekļuves faktu un veic nepieciešamos drošības pasākumus turpmāku drošības incidentu novēršanai.

V Informācijas nodošana citām valsts amatpersonām

28. Augstskola likumā noteiktajos gadījumos izpauž personas datus valsts un pašvaldību amatpersonām. Personas datus izpauž tikai tām valsts un pašvaldību amatpersonām, kuras pirms datu izpaušanas ir identificējusi.

29. Personas datus šo Noteikumu 28.punktā minētajām personām ir tiesības izpaust, pamatojoties uz rakstveida iesniegumu vai vienošanos, norādot datu izmantošanas mērķi, ja likumā nav noteikts citādi. Personas datu pieprasījumā norādāma informācija, kas ļauj identificēt datu pieprasītāju un datu subjektu, kā arī pieprasāmo personas datu apjomus.

VI Rīcība drošības incidentu un avāriju gadījumā

30. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) Lietotājam ir nekavējoties jāziņo šo Noteikumu 8. punktā minētajai atbildīgajai personai, vai tās pilnvarotām personām.

31. Lietotājam ir jāziņo nekavējoties šo Noteikumu 8. punktā minētajai atbildīgajai personai vai viņa pilnvarotai personai par gadījumiem, kad trešajai personai kļuvis zināms pieejas kods videonovērošanas tehnikai.

32. Augstskola, saņemot informāciju par iespējamu drošības incidentu personas datu aizsardzībā, nekavējoties nodrošina drošības incidenta izmeklēšanu, kompetentu valsts iestāžu informēšanu, ja nepieciešams, un nodrošinātu nepieciešamu preventīvu darbību veikšanu personas datu drošības nodrošināšanai atbilstoši tiesību aktu prasībām.