LATVIJAS REPUBLIKA
IZGLĪTĪBAS UN ZINĀTNES MINISTRIJA

PROFESIONĀLĀS IZGLĪTĪBAS KOMPETENCES CENTRS
„DAUGAVPILS TEHNIKUMS"

Reģ. Nr. 2734003068, Strādnieku ielā 16, Daugavpilī, LV–5404
Tālrunis/fakss 65436893, 27741511, e-pasts: dvt@daugvt.lv, www.daugvt.lv

IEKŠĒJIE NOTEIKUMI

Daugavpilī

21.09.2020. Nr. 1.6/11

Datu aizsardzības politika

Izdots saskaņā ar Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 2.punktu, Ministru kabineta noteikumiem „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām"

1. Personas datu apstrādi regulējošie normatīvo aktu un standartu saraksts:

Drošības standarti (rekomendējoši):

ISO/IEC 17799:2005;
ISO/IEC 27001:2005.

Eiropas Savienības normatīvie akti:

- Eiropas Parlamenta un Padomes Regula Nr. 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

Latvijas Republikas normatīvie akti:

- Fizisko personu datu apstrādes likums (Izsludināts 2018. gada 4. jūlijā);
- Ministru kabineta 2015. gada 28. jūlija noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".

2. Terminu skaidrojums:

Izglītības iestāde/ Pārzinis	Profesionālās izglītības profesionālas centrs „DAUGAVPILS TEHNIKUMS" reģistrācijas numurs 2734003068
VDAR (Vispārīgā datu aizsardzības regula)	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

Personas dati	Jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjekts"); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;
Apstrāde	Jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;
Pārzinis	Fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus; ja šādas apstrādes nolūkus un līdzekļus nosaka ar Savienības vai dalībvalsts tiesību aktiem, pārzini vai tā iecelšanas konkrētos kritērijus var paredzēt Savienības vai dalībvalsts tiesību aktos;
Apstrādātājs	Fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus;
Ierobežotas pieejamības informācija	Jebkāda informācijas, kas attiecas uz uzņēmuma komercnoslēpumu, uzņēmuma finanšu informāciju, cilvēkresursiem, biznesa modeļiem, uzņēmuma konfidenciālo informāciju, fizisko personu datiem, to apstrādes nolūkiem un veidiem, datu kategorijām, apstrādes metodēm.

3. Vispārējas noteikumi

3.1. Pārziņa datu aizsardzības politika (turpmāk – politika) nosaka personas datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības, nodrošinot fizisko personu datu apstrādes drošību atbilstoši Vispārīgās datu aizsardzības regulas (turpmāk – VDAR) noteiktajām prasībām.

3.2. Politikas mērķis ir noteikt pārziņa organizatorisko pasākumu un nepieciešamo tehnisko līdzekļu kopumu, kas nodrošina godprātīgu un likumīgu personas datu apstrādi un lietošanu tikai paredzētajiem nolūkiem, to glabāšanas, atjaunošanas, labošanas un dzēšanas veidu, nodrošinot ikvienas fiziskas personas tiesības uz savu personas datu aizsardzību.

3.3. Personas datu apstrāde tiek veikta pārziņa biroja telpās un/ vai pārziņa pārvaldībā esošajās informācijas sistēmās (turpmāk – IS).

3.4. Politikas noteikumi attiecas tikai uz tiem pārziņa darbiniekiem, kuri apstrādā personas datus. Politikas noteikumi attiecināmi uz visiem personas datiem, kas attiecas uz identificētu vai identificējamu fizisko personu.

3.5. Personas datu obligāto tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret drošības incidentu radītu personas datu apdraudējumu.

3.6. Dati, kas tiek izmantoti personas datu apstrādē, ir klasificējami kā ierobežotas pieejamības informācija, kas paredzēta tikai noteiktam pārziņa darbinieku lokam.

4. IS drošības politika

4.1. IS drošības politikas mērķi un pamatnostādnes

4.1.1. Pārziņa informācijas drošības politika (turpmāk – drošības politika) ir izstrādāta un tiek īstenota saskaņā ar pārziņa darbības mērķiem un uzdevumiem, Eiropas Savienības un Latvijas Republikā spēkā esošajiem normatīvajiem aktiem un starptautisko IS drošības standartu rekomendāciju.

4.1.2. Drošības politika ir izstrādāta ar mērķi nodrošināt tādu informācijas tehnoloģiju vidi, lai pārziņa informācijas un tehnoloģiskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības riskiem un vienlaikus nodrošinātu Pārziņa nepārtrauktu un kvalitatīvu darbību atbilstoši normatīvajos aktos noteiktajām funkcijām.

4.1.3. Drošības politika nosaka galvenos drošības pamatnosacījumus informācijas tehnoloģiju videi un nosaka kārtību informācijas un tehnoloģisko resursu aizsardzības nodrošināšanai.

4.1.4. Drošības politika ir saistoša visiem pārziņa un tā iestāžu darbiniekiem, kā arī tiem ārpakalpojumu sniedzējiem, kuri pārzinim sniedz ar IT saistītus pakalpojumus.

4.2. Drošības politikas īstenošanas pamatprincipi

4.2.1. Noteikt un patstāvīgi pilnveidot dokumentu un pasākumu kopumu, kuru īstenošana nodrošina drošības politikas mērķa sasniegšanu.

4.2.2. Risku ierobežošanas un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties šo risku īstenošanas vai pārziņa darbības pārtraukšanas gadījumos.

4.2.3. Tiek sekmēta katra darbinieka izpratne par pienākumiem risku un darbības nepārtrauktības pārvaldīšanā, kā arī informācijas un tehnoloģisko resursu aizsardzības nodrošināšanā, veicot pārziņa darbinieku regulāru izglītošanu.

4.2.4. Tiek nodrošināta pastāvīga drošības politikas īstenošanas koordinēšana un pārraudzīšana.

4.2.5. Gadījumos, kad darbinieki neievēro IS drošības politikas izvirzītās prasības, pārzinis, pamatojoties uz normatīvajiem aktiem, var ierosināt disciplināratbildības procesu.

4.3. Drošības organizācija

4.3.1. **Pārziņa vadība.** Pārziņa vadība kopumā ir atbildīga par informācijas drošības politikas īstenošanu, t.sk. atbildīga par IT drošības organizācijas izveidi un atbildības noteikšanu, kontroles noteikšanu un adekvātu resursu piešķiršanu IT drošības organizācijas pilnvērtīgai funkcionēšanai.

4.3.2. **Datu aizsardzības speciālists.** Lai nodrošinātu konkrētu drošības pasākumu īstenošanu un koordināciju kopumā, pārziņa vadītājs nozīmē datu aizsardzības speciālistu, kurš ir tieši pakļauts pārziņa vadībai. Datu aizsardzības speciālists atbild par risku analīzes veikšanu, nepieciešamo IS drošības normatīvās bāzes uzturēšanu un īstenošanu, noteikto drošības prasību ievērošanas uzraudzību, IT drošības incidentu izmeklēšanu un darbinieku apmācību informācijas drošības jomā.

4.3.3. **Informācijas lietotājs**. Informācijas lietotājs ir atbildīgs par visām darbībām, kuras ir veiktas ar viņa lietotāja vārdu. Informācijas lietotājam ir pienākums informēt datu aizsardzības speciālistu par visiem IT drošības pārkāpumiem un aizdomīgiem notikumiem.

4.3.4. **IS audits.** IS audita uzdevums ir novērtēt drošības prasību izpildi. Nepieciešamības gadījumā, bet ne retāk kā reizi gadā, auditam ir jāveic IS drošības audits. Drošības auditu var veikt piesaistot ārpakalpojuma sniedzēju.

4.4. Informācijas klasifikācija

4.4.1. Informācijas klasifikācijas mērķis ir apzināt visas pārziņa rīcībā esošās informācijas nozīmību un nodrošināt katras informācijas grupas aizsardzību atbilstoši tās klasifikācijas līmenim.

4.4.2. Informācijas resursu turētāji veic informācijas resursu klasificēšanu pēc to vērtības, konfidencialitātes un pieejamības.

4.4.3. Informācijas klasifikācija attiecas uz visu informāciju neatkarīgi no informācijas nesēja.

4.4.4. Informāciju pēc konfidencialitātes pakāpes, vērtējot draudus tās nesakcionētai noplūdei, klasificē šādi:

4.4.4.1. vispārpieejamā informācija;

4.4.4.2. ierobežotas pieejamības informācija.

4.4.5. Informāciju, vērtējot draudus informācijas integritātei, klasificē pēc vērtības līmeņa, šādi:

4.4.5.1. augsti vērtīga informācija;

4.4.5.2. vidēji vērtīga informācija.

4.4.6. Informāciju pēc pieejamības līmeņa, nosakot pieļaujamo laiku, kurā informācijas resursi var nebūt pieejami, kad tiek vērtēti draudi tās pieejamībai klasificē šādi:

4.4.6.1. nepārtrauktas pieejamības informācija;

4.4.6.2. fiksēts pieejamības informācija (piemēram, pieejama tikai darba laikā).

4.4.7. Informācija, kura nav klasificēta atbilstoši konfidencialitātes principiem automātiski tiek uzskatīta par ierobežotas pieejamības informāciju.

4.4.8. Ja datu nesējā glabājas dažādu līmeņu klasificētā informācija, kā kopīgo datu nesēja klasifikācijas līmeni norāda augstāko šajā nesējā esošās informācijas līmeni.

4.4.9. Visiem ierobežotas pieejamības informācijas nesējiem jābūt attiecīgai atzīmei par informācijas klasifikāciju.

4.5. Risku analīze un risku pārvaldības plāns

4.5.1. Ņemot vērā informācijas resursu klasifikāciju, tiek veikta risku pārvaldīšana. Lai plānotu risku pārvaldīšanas pasākumus, datu aizsardzības speciālists sadarbojoties ar struktūras vadītājiem veic IS risku analīzi.

4.5.2. Risku analīzes mērķis ir novērtēt:

4.5.2.1. IS apdraudējuma varbūtību, kur IS apdraudējums ir ar nodomu vai aiz neuzmanības izdarīta darbība vai bezdarbība, vai iespējama notikuma, kas var izraisīt informācijas dzēšanu noklusēšana, informācijas resursu vai tehnoloģisko resursu maiņu, bojāšanu vai informācijas nonākšanu nepilnvarotu personu rīcībā;

4.5.2.2. iespējamo kaitējumu informācijas resursu turētājam vai pārzinim, ja nav nodrošināta informācijas sistēmas drošība.

4.5.3. Risku analīzi periodiski veic visām IS, kā arī katram jaunam ar IS saistītam projektam un IS, kurām veiktas izmaiņas, kas var ietekmēt IS drošību. Analizējot riskus, ņem vērā aktuālāko situāciju attiecībā uz IS aizsardzības pasākumiem.

4.5.4. Risku analīzi veic, lietojot pārziņa noteikto risku analīzes metodoloģiju.

4.5.5. Saskaņā ar risku analīzes rezultātiem tiek sagatavots risku pārvaldības plāns par drošības līdzekļu ieviešanu.

4.5.6. IS drošības riska pārvaldības plānā ietverams informācijas sistēmu drošības risku uzskaitījums un izvērtējums, pasākumu apraksts, izpildes termiņš, finansējums un par izpildi atbildīgo personu saraksts.

4.6. Kopējā risku pārvaldība

4.6.1. Vispārējie drošības jautājumi:

4.6.1.1. tehnoloģisko resursu turētājs seko informācijai par aparatūras un programmatūras jauninājumiem, lai novērstu IS drošības trūkumus, par kuriem ir publicēta informācija. Tehnoloģisko resursu turētājs apkopo informāciju par IS kļūdām, lietotāju jautājumiem un citām problēmām;

4.6.1.2. vispārējais datu uzglabāšanas režīms, kas tiek nodrošināts Pārziņa datortīklā, atbilst vidējas vērtības iekšējas lietošanas informācijas statusam ar pieejamību darba laikā;

4.6.1.3. darbiniekiem, kas veic IS pārvaldību, nosaka pienākumus, atbildību un nodrošina savstarpējo aizvietojamību.

4.7. Fiziskā aizsardzība

4.7.1. Risku pārvaldīšanas ietvaros realizē IS fiziskās aizsardzības pasākumus, kas aizsargā no nevēlamiem apkārtējās vides (ugunsgrēks, plūdi, temperatūras svārstības u.c.), tehniskajiem (neatbilstoša elektroenerģijas padeve u.c.) un cilvēkfaktoriem (tīši vai netīši bojājumi, zādzība u.c.).

4.7.2. IS fiziskās aizsardzības pasākumi detalizēti tiek aprakstīti informācijas sistēmu iekšējos drošības noteikumos. Atbildīgais par sistēmu iekšējo drošības noteikumu izstrādi ir datu aizsardzības speciālists.

4.8. Loģiskā aizsardzība

4.8.1. Risku pārvaldīšanas ietvaros realizē IS loģiskās aizsardzības pasākumus.

4.8.2. IS loģiskās aizsardzības pasākumi detalizēti tiek aprakstīti informācijas sistēmu iekšējos drošības noteikumos.

4.9. IS darbības nepārtrauktības un avārijas atjaunošanas plānošana un pārvaldība

4.9.1. Lai nodrošinātu informācijas sistēmu darbības nepārtrauktību un avārijas atjaunošanu, jāizstrādā IS darbības nepārtrauktības un atjaunošanas plāns.

4.9.2. Atbildīgais par IS darbības nepārtrauktības un atjaunošanas plāna izstrādi un uzturēšanu ir tehnoloģisko resursu turētājs.

4.9.3. IS darbības nepārtrauktības un atjaunošanas plānā ir jāietver pasākumu apraksts sistēmu nepārtrauktai darbībai un to atjaunošanai avārijas gadījumā.

4.9.4. IS darbības nepārtrauktības pārvaldīšanas ietvaros tehnoloģisko resursu turētāji veic šādus pasākumus:

4.9.4.1. identificē visas būtiskās IS darbības funkcijas, kuras nodrošina IS;

4.9.4.2. nosaka prioritātes līmeņus atjaunojamajām funkcijām atkarībā no to svarīguma darbības veikšanai un zaudējumu samazināšanai;

4.9.4.3. sadarbībā ar informācijas turētājiem nosaka IS nepārtrauktības prasības.

4.9.5. Prasību izveidošanā jāizmanto IS klasifikācijā iegūtā informācija:

4.9.5.1. identificē apdraudējumus, kas var pārtraukt vai bojāt IS darbību;

4.9.5.2. nosaka darbības atjaunošanas vai aizstāšanas prasības katrai funkcijai un IS, kura šo funkciju nodrošina.

4.9.6. Tehnoloģisko resursu turētājs veic IS darbības atjaunošanas plāna izstrādi, uzturēšanu, testēšanu un realizēšanu vai nosaka rakstiski, kurš darbinieks to veic.

4.9.7. Tehnoloģisko resursu turētājs organizē regulāru (ne retāk kā reizi gadā) IS darbības atjaunošanas procesos iesaistīto personu apmācību un plāna testēšanu, lai pārliecinātos par tā darbību.

Direktore I. Brokāne