					Šeit ievadiet reģistrētās juridiskās personas nosaukumu						
Dokumenta numurs: P08					Dokumenta nosaukums: **Informācijas drošības informētības un apmācību politika**						
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:						
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	7. punkts 7.3, A pielikuma 6. kontrole 6.3	Nosaka informētības un apmācību prasības, kas ir ietvertas šajā politikā
ISO/IEC 27002:2022	6. kontrole	Atbalsta amata lomai atbilstošu informētības apmācību
NIST SP 800-53 Rev.5	AT-1 līdz AT-5	Saskaņots ar politikām un procedūrām, informētības apmācību, uz lomām balstītu apmācību, apmācību ierakstiem un saziņu ar drošības komandu
EU GDPR	32., 39. pants; 78. apsvērums	Nosaka pienākumu nodrošināt apmācību personas datu apstrādē iesaistītajiem darbiniekiem un vispārēju personāla informētību
EU NIS2	21. panta 2. punkta a) un b) apakšpunkts, 21. panta 3. punkts	Pieprasa risku un drošības apmācību politikas un informētības iniciatīvas
EU DORA	5., 8., 13. pants	Pieprasa IKT risku informētību un apmācību kā daļu no noturības kontroles pasākumiem
COBIT 2019	APO07, DSS05, MEA	Pastiprina darbaspēka informētību, lietotāju izglītošanu un atbilstības uzraudzību

1. Mērķis

1.1 Šī politika nosaka formālu ietvaru, lai nodrošinātu, ka viss personāls apzinās savus informācijas drošības pienākumus un saņem apmācību, kas nepieciešama informācijas aktīvu konfidencialitātes, integritātes un pieejamības (CIA) aizsardzībai.

1.2 Tā atbalsta ISO/IEC 27001 7.3. punkta un A pielikuma 6. kontroles 6.3 prasības, nosakot strukturētu, uz risku balstītu informētības un apmācību programmu, kas pielāgota organizācijas lomām un mainīgajiem apdraudējumiem.

1.3 Politika veicina ar cilvēkfaktoru saistīto ievainojamību mazināšanu, drošību apzinošas uzvedības stiprināšanu un drošu prakšu nepārtrauktu nostiprināšanu atbilstoši normatīvajām prasībām un līgumsaistībām.

2. Tvērums

2.1 Šī politika attiecas uz visām iekšējām un ārējām personām, kurām ir piekļuve organizācijas informācijas sistēmām, datiem vai telpām, tostarp:

2.1.1 darbiniekiem (pilnas slodzes, nepilnas slodzes, pagaidu darbinieki);

2.1.2 līgumslēdzējiem un trešo personu pakalpojumu sniedzējiem, konsultantiem, piegādātājiem un praktikantiem;

2.1.3 trešajām pusēm ar loģisku vai fizisku piekļuvi saskaņā ar pakalpojumu līmeņa vienošanos.

2.2 Tvērumā ietilpst:

2.2.1 sākotnējā drošības informētības ievadapmācība;

2.2.2 lomai specifiska apmācība (piemēram, izstrādātājiem, finanšu personālam, lietotājiem ar privileģētiem kontiem);

2.2.3 periodiska atkārtota apmācība un informētības kampaņas;

2.2.4 ad hoc apmācība, reaģējot uz incidentiem vai jauniem apdraudējumiem.

2.3 Šīs politikas ietvaros aptvertās apmācību nodrošināšanas metodes ietver e-apmācības, klātienes instruktāžas, simulācijas, zināšanu pārbaudes, plakātus, drošības biļetenus un obligātus apliecinājumus.

3. Mērķi

3.1 Nodrošināt, ka viss personāls izprot savus pienākumus organizācijas aktīvu aizsardzībā un drošības politiku ievērošanā.

3.2 Nodrošināt pastāvīgu, izmērāmu informētības apmācību, kas ir saskaņota ar uz lomām balstītu riska pakļautību.

3.3 Iekļaut drošu uzvedību ikdienas darbībās, nostiprinot tādas prakses kā droša paroļu izmantošana, ziņošana par incidentiem un noturība pret pikšķerēšanu.

3.4 Nodrošināt normatīvo prasību ievērošanu un gatavību auditam attiecībā uz informācijas drošības apmācību prasībām dažādās nozarēs un jurisdikcijās.

3.5 Samazināt drošības incidentus, kas izriet no nolaidības, informētības trūkuma vai kļūdainiem spriedumiem, izmantojot uzvedības nostiprināšanu un nepārtrauktu atkārtošanu.

4. Lomas un atbildība

4.1 Izpildvadība

4.1.1 Apstiprina organizācijas informācijas drošības apmācību stratēģiju un nodrošina, ka tai ir piešķirti resursi un tā ir iekļauta uzņēmuma prioritātēs.

4.1.2 Vadības līmenī uzrauga atbilstību un nodrošina politikas ievērošanu visās struktūrvienībās.

4.2 Galvenais informācijas drošības vadītājs / IDPS vadītājs

4.2.1 Ir šīs politikas īpašnieks un nosaka informētības un apmācību ietvaru atbilstoši riskam, atbilstības prasībām un biznesa vajadzībām.

4.2.2 Uzrauga visu drošības apmācību iniciatīvu izstrādi, īstenošanu, uzskaiti un pārskatīšanu.

4.2.3 Nodrošina, ka apmācības tiek periodiski atjauninātas un atspoguļo mainīgos apdraudējumus un jaunās tehnoloģijas.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Pārskatīšanas biežums

9.1.1 Šī politika un saistītā apmācību programma ir jāpārskata:

9.1.1.1 reizi gadā, vai

9.1.1.2 pēc būtiskiem incidentiem, kas saistīti ar cilvēkfaktora kļūdām vai iekšējiem apdraudējumiem;

9.1.1.3 ieviešot būtiskas jaunas tehnoloģijas vai saskaroties ar jauniem apdraudējumiem;

9.1.1.4 reaģējot uz izmaiņām tiesiskajās, līgumiskajās vai sertifikācijas prasībās.

9.2 Pārskatīšanas process

9.2.1 Pārskatīšanu vada galvenais informācijas drošības vadītājs sadarbībā ar:

9.2.1.1 personāla nodaļu un apmācību struktūrvienībām;

9.2.1.2 juridisko funkciju, atbilstības funkciju un datu aizsardzības speciālistu;

9.2.1.3 IT drošības un operacionālā riska funkcijām.

9.2.2 Visi atjauninājumi ir:

9.2.2.1 jāapstiprina informācijas drošības vadības komitejai;

9.2.2.2 jāpārvalda ar versiju kontroli un jādokumentē IDPS dokumentu reģistrā;

9.2.2.3 jāpaziņo lietotājiem, ja būtiskas izmaiņas ietekmē apmācību tvērumu vai pienākumus.

9.3 Satura atjaunināšanas pārvaldība

9.3.1 Apmācību moduļi un informētības materiāli ir jāpārskata ik pēc 12 mēnešiem, lai nodrošinātu:

9.3.1.1 atbilstību apdraudējumu videi;

9.3.1.2 normatīvo precizitāti;

9.3.1.3 formāta savietojamību (piemēram, pieejamību, lokalizāciju).

9.3.2 Novecojis vai maldinošs saturs ir nekavējoties jāatsauc un jāaizstāj ar apstiprinātām alternatīvām.

10. Saistītās politikas un sasaistes

10.1 Šo politiku atbalsta un tās ievērošanu papildina:

10.1.1 P01 – Informācijas drošības politika: nosaka drošības informētību kā pamatkontroles pasākumu organizācijas IDPS.

10.1.2 P03 – Pieļaujamās lietošanas politika: pieprasa lietotāja apliecinājumu apmācību laikā un precizē pienākumus, kas saistīti ar tehnoloģiju ikdienas izmantošanu.

10.1.3 P07 – Darba attiecību uzsākšanas un izbeigšanas politika: nodrošina, ka apmācība ir iekļauta uzsākšanas posmā un tiek uzraudzīta visā nodarbinātības laikā.

10.1.4 P06 – Risku pārvaldības politika: sasaista uz cilvēkfaktoru vērstu apmācību ar draudu modelēšanu un atlikušā riska samazināšanas stratēģijām.

10.1.5 P33 – Audita un atbilstības uzraudzības politika: validē, ka informētības kontroles pasākumi auditu laikā ir ieviesti, izmērāmi un efektīvi.

10.2 Kopā šīs politikas veido visaptverošu uzvedības kontroles ietvaru, kas apvieno informētību, pārskatatbildību un kultūras nostiprināšanu.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 7. punkts 7.3 – Informētība: pieprasa organizācijām nodrošināt, ka darbinieki apzinās informācijas drošības politikas un savus pienākumus. Šī politika ievieš šo prasību praksē, izmantojot strukturētu ievadapmācību, periodisku apmācību un izmērāmu dalību kampaņās.

11.1.2 A pielikuma 6. kontrole 6.3 – Informācijas drošības informētība, izglītošana un apmācība: pilnībā nodrošināta ar sākotnējām, uz lomām balstītām un nepārtrauktām apmācību programmām, kas pielāgotas lietotāju riska profiliem.

11.2 ISO/IEC 27002:2022 – 6. kontrole

11.2.1 Atbalsta amata lomām atbilstošas informētības apmācības izstrādi un nodrošināšanu, uzsverot drošas uzvedības nostiprināšanu un periodiskus atjauninājumus, pamatojoties uz apdraudējumu izlūkošanu un audita atgriezenisko saiti.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 līdz AT-5 (informētības un apmācību saime): šī politika ir saskaņota ar AT-1 (politika un procedūras), AT-2 (informētības apmācība), AT-3 (uz lomām balstīta apmācība), AT-4 (drošības apmācību ieraksti) un AT-5 (saziņa ar drošības grupām).

11.3.2 IA-5, AC-2: nostiprina lietotāja atbildību par drošu autentifikāciju un pieļaujamo lietošanu — tas ir informētības programmu uzvedības rezultātu pamats.

11.3.3 IR-1 līdz IR-8: gatavība reaģēšanai uz incidentiem tiek stiprināta ar mērķētām informētības kampaņām un simulācijām.

11.4 EU GDPR (2016/679)

11.4.1 32. pants – apstrādes drošība: nosaka, ka personālam, kas apstrādā personas datus, jābūt apmācītam atpazīt, novērst un ziņot par riskiem personas datiem. Šī politika nodrošina, ka personas datu apstrādē iesaistītie darbinieki un visas attiecīgās lomas tiek atbilstoši apmācītas.

11.4.2 39. pants – datu aizsardzības speciālista uzdevumi: ietver informētības veicināšanu un personāla apmācību, kas iesaistīts apstrādes darbībās.

11.4.3 78. apsvērums: veicina atbilstošus informētības pasākumus, lai nodrošinātu stingras drošības prakses un politikas ievērošanu.

11.5 EU NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta a) un b) apakšpunkts: pieprasa organizācijām pieņemt politikas par riska analīzi un drošības apmācību visam attiecīgajam personālam. Šī politika izpilda šo prasību, nosakot nepārtrauktus, lomai pielāgotus apmācību procesus.

11.5.2 21. panta 3. punkts: veicina kiberdrošības risku informētību vadības un personāla vidū, izmantojot informētības iniciatīvas un simulācijas.

11.6 EU DORA (2022/2554)

11.6.1 13. pants – digitālās darbības noturības stratēģija: nosaka, ka IKT risku informētībai un apmācībai jābūt daļai no pārvaldības modeļa. Šī politika nodrošina, ka cilvēkfaktora risks tiek pārvaldīts ar nepārtrauktu izglītošanu un apdraudējumu simulācijām.

11.6.2 5. un 8. pants: uzsver iekšējās kontroles ietvaru nozīmi, kuros informētība un apmācība ir pamatkomponenti IKT noturībai un kiberdrošības higiēnai.

11.7 COBIT 2019

11.7.1 APO07 – Pārvaldīti cilvēkresursi: pastiprina nepieciešamību attīstīt izpratni par drošības pienākumiem un integrēt to darbaspēka pārvaldībā.

11.7.2 DSS05 – Pārvaldīti drošības pakalpojumi: nosaka kontroles pasākumus lietotāju izglītošanai un ziņošanai par incidentiem, kas abi ir šīs politikas neatņemama daļa.

11.7.3 MEA03 – Atbilstības uzraudzība, izvērtēšana un novērtēšana: pieprasa pārskatīt lietotāju uzvedības un politikas ievērošanas efektivitāti — šajā politikā tas tiek īstenots ar pikšķerēšanas testiem, testiem un informētības kampaņu metriku.