					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P08S					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	
ISO/IEC 27002:2022	6. kontrole	
NIST SP 800-53 Rev.5	AT-2, AT-4	
NIS2 direktīva	21. panta 2. punkta i) apakšpunkts	
DORA	13. pants	
COBIT 2019	BAI08, DSS	
GDPR	32., 39. pants	

1. Mērķis

1.1. Šī politika nodrošina, ka visi darbinieki un līgumslēdzēji izprot savus pienākumus informācijas drošības jomā.

1.2. Tās mērķis ir samazināt cilvēcisku kļūdu iespējamību, uzlabot spēju atklāt incidentus un ziņot par tiem, kā arī veicināt drošības izpratni visā organizācijā.

1.3. Šī politika nodrošina atbilstību ISO/IEC 27001, NIS2, GDPR un DORA prasībām, integrējot drošības informētību ikdienas darba praksē un amata pienākumos.

2. Tvērums

2.1. Šī politika attiecas uz visiem darbiniekiem, līgumslēdzējiem, praktikantiem un trešajām personām, kurām ir piekļuve uzņēmuma sistēmām vai datiem.

2.2. Tā ietver:

2.2.1. sākotnējo ievadapmācību jaunajiem darbiniekiem;

2.2.2. ikgadējo atkārtoto drošības apmācību;

2.2.3. ad hoc informētības pasākumus (piemēram, ar incidentiem saistītus paziņojumus, plakātus vai ieteikumus).

2.3. Politika ir piemērojama visām lomām, struktūrvienībām un darba vietām.

3. Mērķi

3.1. Nodrošināt, ka viss personāls savlaicīgi saņem saprotamu un atbilstošu drošības informētības apmācību.

3.2. Nodrošināt darbiniekiem spēju atpazīt un novērst izplatītus apdraudējumus, piemēram, pikšķerēšanu, ļaunprogrammatūru un datu noplūdes.

3.3. Nodrošināt apmācību pabeigšanas dokumentēšanu, lai pierādītu atbilstību tiesiskajām, līgumiskajām un audita prasībām.

3.4. Uzturēt aktuālu apmācību saturu, kas atspoguļo organizācijas politikas, apdraudējumus un piemērojamās prasības.

3.5. Veicināt personāla proaktīvu pieeju, kurā drošība tiek uzskatīta par ikdienas pienākumu sastāvdaļu.

4. Lomas un atbildība

4.1. Ģenerāldirektors

4.1.1. Apstiprina apmācību prasības un nodrošina nepieciešamo resursu piešķiršanu.

4.1.2. Pārskata apmācību izpildes pārskatus un nepieciešamības gadījumā eskalē neatbilstības.

4.2. Biroja vadītājs / personāla vadība

4.2.1. Koordinē apmācību nodrošināšanu jaunpieņemtajiem darbiniekiem un ikgadējai atkārtotajai apmācībai.

4.2.2. Uztur apmācību ierakstus un izpildes žurnālus.

4.2.3. Nodrošina personāla apliecinājumus par galvenajām informācijas drošības politikām un konfidencialitātes līgumu.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Ikgadējā pārskatīšana

9.1.1. Šī politika reizi gadā ir jāpārskata ģenerāldirektoram un personāla vadībai, lai nodrošinātu tās atbilstību aktuālajiem riskiem, prasībām un personāla vajadzībām.

9.2. Starplaika atjauninājumi

9.2.1. Politika un apmācību saturs ir jāpārskata un jāgroza arī pēc:

9.2.1.1. būtiska drošības incidenta;

9.2.1.2. tiesiskām vai līgumiskām izmaiņām;

9.2.1.3. organizatoriskas pārstrukturēšanas vai sistēmu migrācijas.

9.3. Versiju kontrole un izplatīšana

9.3.1. Katrā atjauninājumā ir jāiekļauj:

9.3.1.1. versijas numurs un spēkā stāšanās datums;

9.3.1.2. izmaiņu kopsavilkums;

9.3.1.3. ģenerāldirektora apstiprinājums;

9.3.1.4. visu iepriekšējo versiju arhīvs, kas jāglabā vismaz trīs gadus.

9.4. Darbinieku informēšana

9.4.1. Politikas atjauninājumi ir jāpaziņo visam personālam, un, ja ir veiktas būtiskas izmaiņas, ir jāsaņem apliecinājums.

10. Saistītās politikas un sasaistes

10.1. Šī politika atbalsta šādas politikas:

10.1.1. P2S – Pārvaldības lomu un atbildības politika: nosaka atbildību par apmācību koordinēšanu un uzraudzību.

10.1.2. P3S – Pieļaujamās lietošanas politika: nostiprina apmācībā ietvertās uzvedības prasības.

10.1.3. P4S – Piekļuves kontroles politika: nodrošina, ka lietotāji izprot piekļuves drošības nozīmi.

10.1.4. P7S – Darba attiecību uzsākšanas un izbeigšanas politika: integrē apmācību ievadprocesā.

10.1.5. P30S – Incidentu reaģēšanas politika: nodrošina, ka personāls zina, kā savlaicīgi un pareizi ziņot par incidentiem.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. 7.3. punkts – nosaka, ka organizācijām jānodrošina personāla informētība par viņu pienākumiem un ietekmi uz drošību.

11.2. ISO/IEC 27002

11.2.1. 6.3. kontrole – detalizē prasības attiecībā uz drošības apmācību tvērumu un nodrošināšanu.

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – nosaka prasību nodrošināt informētības apmācību lietotājiem ar piekļuvi sistēmām.

11.3.2. AT-4 – aptver uz lomām balstītu apmācību un neatbilstības sekas.

11.4. GDPR

11.4.1. 32. pants – nosaka drošības pasākumus, tostarp personāla apmācību, personas datu aizsardzībai.

11.4.2. 39. pants – nosaka, ka, kur piemērojams, datu aizsardzības speciālists uzrauga informētību un apmācību.

11.5. NIS2 direktīva

11.5.1. 21. panta 2. punkta i) apakšpunkts – nosaka nepārtrauktas kiberdrošības informētības un apmācību programmas.

11.6. DORA

11.6.1. 13. pants – nosaka finanšu nozares subjektiem pienākumu ieviest izglītošanu un apmācību visam personālam ar IKT saistītiem pienākumiem.

11.7. COBIT 2019

11.7.1. BAI08 – Pārvaldīt zināšanas: nodrošina, ka personāls ir kompetents un apmācīts.

11.7.2. DSS05 – Pārvaldīt drošības pakalpojumus: uzsver informētību kā būtisku drošības kontroles pasākumu.