					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P03					Dokumenta nosaukums: **Pieņemamas lietošanas 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**

Saskaņotība ar standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	5. kontroles pasākums	Nosaka uzvedības normas un prasības pieņemamas lietošanas politikai
ISO/IEC 27002:2022	Kontroles pasākumi 6.1, 6.2, 8.1, 8.12	Nosaka informācijas drošības pienākumus, informētību, kā arī ierīču un datu pārvaldību
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Piekļuves kontroles un informētības/uzvedības kontroles pasākumi, kas attiecas uz IT aktīvu lietošanu
ES VDAR	5. panta 1. punkta f) apakšpunkts, 32. pants; apsvērums 39	Nosaka konfidencialitātes un integritātes prasības, tehniskos un organizatoriskos kontroles pasākumus, kā arī tiesisko pamatu pienācīgai lietošanai
ES NIS2	21. panta 2. punkta a)–d) apakšpunkts	Nosaka prasību pēc operacionālajām politikām un drošas lietošanas apmācības
ES DORA	5. pants	Atbalsta IKT riska pārvaldību, reglamentējot lietotāju rīcību
COBIT 2019	APO07, BAI05, DSS05, MEA01	Personālvadība, pārmaiņu pārvaldība, drošības pārvaldība, atbilstības un veiktspējas uzraudzība

1. Mērķis

1.1 Šī politika nosaka organizācijas informācijas sistēmu, skaitļošanas resursu, saziņas rīku un datu apstrādes prakses pieņemamu un nepieņemamu lietošanu.

1.2 Tā nodrošina, ka visi lietotāji izprot savus pienākumus, lietojot organizācijas IT aktīvus, un ka viņu darbības atbalsta informācijas konfidencialitāti, integritāti, pieejamību un tiesisku apstrādi.

1.3 Šī politika izpilda ISO/IEC 27001:2022 5.10. kontroles pasākuma prasību, nosakot sistēmu lietošanas uzvedības normas un ieviešot tehniskos un procesuālos kontroles pasākumus, lai mazinātu nepareizas lietošanas, nolaidības vai ļaunprātīgas izmantošanas risku.

1.4 Tā arī atbalsta izmeklēšanas un politikas piemērošanas darbības, tostarp reaģēšanu uz incidentiem un disciplināro pasākumu piemērošanu pārkāpumu gadījumā.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām fiziskām un juridiskām personām, kurām piešķirta piekļuve organizācijas informācijas sistēmām un aktīviem, tostarp, bet ne tikai:

2.1.1 Darbiniekiem, līgumdarbiniekiem, konsultantiem, praktikantiem un pagaidu personālam

2.1.2 Trešo pušu piegādātājiem ar piekļuvi sistēmām vai deleģētām administratīvajām lomām

2.1.3 Viesiem vai partneriem, kuri izmanto organizācijai piederošu vai atļautu IT infrastruktūru

2.2 Piemērošanas joma ietver visus organizācijas tehnoloģiju un datu aktīvus, tostarp:

2.2.1 Darbstacijas, klēpjdatorus, mobilās ierīces un serverus

2.2.2 Tīkla infrastruktūru un mākoņpakalpojumus

2.2.3 E-pastu, ziņapmaiņas risinājumus, datņu glabātuves, sadarbības platformas un VPN

2.2.4 Datus glabāšanā, pārsūtē vai apstrādē neatkarīgi no to formāta vai atrašanās vietas

2.2.5 Jebkuru personīgo ierīci, kas tiek izmantota BYOD (Bring Your Own Device) ietvaros un pieslēdzas organizācijas sistēmām

2.3 Šī politika ir piemērojama visās darba vidēs, tostarp:

2.3.1 Organizācijas birojos un ražošanas vietās

2.3.2 Attālinātā darba vietās vai hibrīda darba režīmā

2.3.3 Izbraukuma darbībās vai trešo pušu pārvaldītās telpās

2.4 Piekļuve organizācijas sistēmām vai organizācijas datu apstrāde ir atļauta tikai tad, ja lietotājs ir apliecinājis šīs politikas ievērošanu un to ievēro.

3. Mērķi

3.1 Noteikt un piemērot noteikumus organizācijas IT resursu pieņemamai lietošanai.

3.2 Novērst neatļautu piekļuvi, datu noplūdi vai kaitējumu, kas izriet no nolaidīgas vai ļaunprātīgas lietošanas.

3.3 Aizsargāt organizācijas tīklus, aktīvus un datus no apdraudējumiem, kas rodas lietotāju rīcības dēļ.

3.4 Atbalstīt tiesisko un līgumisko pienākumu izpildi, demonstrējot pienācīgu rūpību IT resursu pārvaldībā.

3.5 Nodrošināt konsekvenci un skaidrību disciplināro pasākumu un izņēmumu pārvaldības procesu piemērošanā.

3.6 Veicināt ētisku, drošu un atbildīgu digitālo un fizisko skaitļošanas resursu lietošanas kultūru.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Apstiprina Pieņemamas lietošanas politiku (AUP) un nodrošina tās atbilstību darbības mērķiem, regulatīvajām prasībām un organizācijas vērtībām.

4.1.2 Piešķir resursus politikas ieviešanai, apmācībām, uzraudzībai un pārskatīšanai.

4.1.3 ISMS pārvaldības ietvaros pārskata atbilstības statusu un disciplināros pasākumus, kas saistīti ar politikas pārkāpumiem.

4.2 IT un informācijas drošības komanda

4.2.1 Ievieš tehniskos kontroles pasākumus šīs politikas piemērošanai, tostarp:

4.2.2 Satura filtrēšanu, aizsardzību pret ļaunprogrammatūru, galiekārtu drošību un tīkla uzraudzības rīkus

4.2.3 E-pasta drošības konfigurācijas un datu zuduma novēršanas (DLP) risinājumus

4.2.4 Bloķēšanas sarakstus un atļauto sarakstus programmatūrai, aparatūrai un tīmekļvietnēm

4.2.5 Uztur apstiprinātās un aizliegtās programmatūras, ierīču un pakalpojumu uzskaiti.

4.2.6 Izmeklē iespējamos AUP pārkāpumus, apkopo digitālās kriminālistikas pierādījumus un, ja nepieciešams, atbalsta disciplināro vai juridisko rīcību.

4.2.7 Sadarbojas ar personāla un juridisko funkciju incidentu apstrādē, eskalācijā un ziņošanas pienākumu izpildē.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Pārskatīšanas ierosinātāji un biežums

9.1.1 Šī politika jāpārskata:

9.1.1.1 Vismaz reizi gadā

9.1.1.2 Pēc jebkurām būtiskām tehnoloģiju vai infrastruktūras izmaiņām

9.1.1.3 Pēc incidentiem vai audita konstatējumiem, kas norāda uz nepilnībām politikas piemērošanā

9.1.1.4 Reaģējot uz izmaiņām piemērojamos tiesību aktos vai līgumos

9.2 Atbildība un apstiprināšana

9.2.1 Par pārskatīšanas procesu ir atbildīgs CISO vai norīkots ISMS vadītājs.

9.2.2 Atjauninājumi jāapstiprina izpildvadībai, un par tiem jāpaziņo visā organizācijā.

9.2.3 Pēc politikas atkārtotas izdošanas atkārtoti jāiegūst apliecinājums par atjaunināto prasību pieņemšanu.

9.3 Dokumentu pārvaldība

9.3.1 Politikā jāiekļauj šādi metadati un versiju pārvaldības dati:

9.3.1.1 Nosaukums, ID un klasifikācijas līmenis

9.3.1.2 Politikas īpašnieks un dokumenta pārzinis

9.3.1.3 Izmaiņu vēsture un atjauninājumu pamatojums

9.3.1.4 Pārskatīšanas datums un nākamais plānotais atjaunināšanas datums

9.3.1.5 Izplatīšanas un apliecinājumu žurnālu atsauces

9.3.2 Galvenā kopija jāglabā ISMS dokumentu repozitorijā versiju kontrolē.

10. Saistītās politikas un savstarpējā saikne

10.1 Šī politika ir interpretējama kopā ar šādām politikām:

10.1.1 P1 – Informācijas drošības politika: nosaka pamatprasības rīcībai un augstākās vadības apņemšanos nodrošināt pieņemamu lietošanu.

10.1.2 P4 – Piekļuves kontroles politika: nosaka atļaujas un tiesības, kas saistītas ar lietotāju, sistēmu un datu piekļuvi, un tieši īsteno pieņemamas lietošanas robežas.

10.1.3 P6 – Risku pārvaldības politika: attiecas uz ar rīcību saistītiem riskiem un atbalsta uzraudzības un apstrādes darbības, kas saistītas ar lietotāju radītiem apdraudējumiem.

10.1.4 P7 – Pieņemšanas darbā un darba attiecību izbeigšanas politika: nodrošina, ka pieņemamas lietošanas nosacījumi tiek apliecināti darba attiecību sākumā un atsaukti to izbeigšanas brīdī.

10.1.5 P9 – Attālinātā darba politika: paplašina pieņemamas lietošanas prasības uz attālinātā un hibrīda darba vidi.

10.2 Šīs saistītās politikas veido daudzslāņainas aizsardzības modeli uzvedības, tehniskās un līgumiskās pārvaldības jomā.

11. Atsauces standarti un ietvari

11.1 Šī Pieņemamas lietošanas politika (AUP) ir saskaņota ar starptautiski atzītiem standartiem un tiesiskajiem ietvariem, lai nodrošinātu piemērojamus, auditējamus un uz risku balstītus uzvedības kontroles pasākumus visā digitālo un fizisko informācijas sistēmu lietošanā.

11.2 ISO/IEC 27001:2022

11.2.1 5.10. kontroles pasākums – Informācijas un citu saistīto aktīvu pieņemama lietošana: šī politika tieši izpilda prasību noteikt, paziņot un piemērot noteikumus, kas reglamentē IT resursu atbilstošu lietošanu.

11.2.2 A pielikuma 6.1. kontroles pasākums – Atbildība par informācijas drošību: nosaka skaidrus pienākumus attiecībā uz lietotāju rīcību un atbilstības pārraudzību.

11.2.3 A pielikuma 6.2. kontroles pasākums – Informācijas drošības informētība, izglītošana un apmācība: apmācības un politikas apliecināšanas procesi ir daļa no AUP piemērošanas.

11.2.4 A pielikuma 8.1. kontroles pasākums – Lietotāju galiekārtas un 8.12. kontroles pasākums – Datu zuduma novēršana: aptver pieņemamu rīcību ar lietotāju ierīcēm un reglamentē darbības, kas var novest pie datu izpaušanas vai noplūdes.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Piekļuves kontrole mobilajām ierīcēm) un AC-20 (Ārējo informācijas sistēmu lietošana): šī politika nosaka lietotāju pienākumus un ierobežojumus attiecībā uz BYOD un trešo pušu sistēmu piekļuvi.

11.3.2 PL-4 (Uzvedības noteikumi): nosaka detalizētas pieņemamas lietošanas prasības, kas atbilst šai politikai.

11.3.3 AT-2 (Drošības informētības apmācība): tiek nodrošināts ar lietotāju apmācībām un dokumentētu politikas apliecināšanu.

11.3.4 AU-2 (Auditējamie notikumi) un AU-12 (Audita ģenerēšana): politikas piemērošana balstās uz lietotāju darbību uzraudzību un brīdinājumiem par pārkāpumiem.

11.4 ES VDAR (2016/679):

11.4.1 5. panta 1. punkta f) apakšpunkts: nosaka personas datu drošību un integritāti; šī politika mazina riskus, ko rada cilvēku rīcība un neatļauta lietošana.

11.4.2 32. pants: nosaka tehniskos un organizatoriskos pasākumus, piemēram, uzvedības kontroles pasākumus un lietošanas ierobežojumus, lai aizsargātu personas datus.

11.4.3 Apsvērums 39: uzsver nepieciešamību nodrošināt tikai nepieciešamo piekļuvi un tiesisku datu lietošanu no pilnvarotu personu puses.

11.5 ES NIS2 direktīva (2022/2555):

11.5.1 21. panta 2. punkta a)–d) apakšpunkts: nosaka prasību pēc operacionālajām politikām un apmācībām drošai sistēmu lietošanai, ko šī AUP nodrošina, definējot rīcību, uzraudzību un politikas piemērošanas procesus.

11.6 ES DORA (2022/2554):

11.6.1 5. pants: šī politika atbalsta IKT riska pārvaldības ietvaru, nosakot noteikumus cilvēka un sistēmas mijiedarbībai un mazinot uzvedībā balstītu kiberrisku ietekmi.

11.7 COBIT 2019:

11.7.1 APO07 – Pārvaldīti cilvēkresursi: nodrošina lietotāju pienākumu un informētības prasības visā darbinieka dzīvesciklā.

11.7.2 BAI05 – Pārvaldītas organizatoriskās pārmaiņas: iekļauj pieņemamas lietošanas pārvaldību izmaiņu procesos, kas ietekmē lietotāju rīcību.

11.7.3 DSS05 – Pārvaldīti drošības pakalpojumi: atbalsta lietotāju darbību uzraudzību, uzvedības brīdinājumus un automatizētus reaģēšanas mehānismus.

11.7.4 MEA01 – Uzraudzīt, izvērtēt un novērtēt veiktspēju un atbilstību: politika nosaka rādītājus un mehānismus, lai apstiprinātu lietotāju atbilstību uzvedības prasībām.