					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P03S					Dokumenta nosaukums: **Pieļaujamās 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. punkts	Attiecas uz politikas vispārējo tvērumu un ieviešanu
ISO/IEC 27002:2022	5.10, 5.11, 5	Vadlīnijas par pieļaujamās lietošanas prasībām un kontroles pasākumiem
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Aptver sistēmu un ierīču lietošanu, uzraudzību un lietotāju apmācību
ES GDPR	5. panta 1. punkta f) apakšpunkts, 32. pants	Datu integritāte, konfidencialitāte un drošības pasākumi
ES NIS2	21. panta 2. punkta b) apakšpunkts	Nosaka pienākumu ieviest atbilstošas drošības un pieļaujamās lietošanas politikas
ES DORA	9. pants	IKT risku pārvaldības politika, kontroles pasākumi un ieviešana
COBIT 2019	DSS05, BAI08	Drošības pakalpojumi un zināšanu pārvaldība

1. Mērķis

1.1. Šī politika nosaka uzņēmuma nodrošināto sistēmu, ierīču, interneta piekļuves, e-pasta, mākoņpakalpojumu un jebkuru uzņēmuma darbībai izmantotu personīgo ierīču pieļaujamu, atbildīgu un drošu lietošanu.

1.2. Tā nodrošina, ka personas izprot savus pienākumus, lietojot organizācijas IT resursus un aizsargājot datu integritāti, privātumu un darbības nepārtrauktību.

1.3. Šī politika atbalsta atbilstību ISO/IEC 27001:2022, nosakot skaidrus lietotāju rīcības standartus, kas atbilst tiesiskajām, līgumiskajām un regulatīvajām prasībām.

2. Tvērums

2.1. Šī politika attiecas uz visām personām, kuras piekļūst uzņēmuma sistēmām vai datiem, tās pārvalda vai ar tām mijiedarbojas, tai skaitā:

2.1.1. darbiniekiem un līgumdarbiniekiem;

2.1.2. pagaidu darbiniekiem un praktikantiem;

2.1.3. ārējiem IT pakalpojumu sniedzējiem.

2.2. Tā aptver:

2.2.1. uzņēmumam piederošus datorus, tālruņus un planšetdatorus;

2.2.2. uzņēmuma darbībai apstiprinātas personīgās ierīces (BYOD);

2.2.3. uzņēmuma tīklus, mākoņplatformas un programmatūras pakalpojumus;

2.2.4. interneta piekļuvi, e-pasta sistēmas, koplietojamās glabātuves un uzņēmuma lietojumprogrammas.

2.3. Šī politika ir piemērojama visās darba vidēs — klātienē, attālināti un hibrīddarba režīmā — un visā darba laikā.

3. Mērķi

3.1. Noteikt, kas ir uzskatāms par pieļaujamu un nepieļaujamu IT sistēmu lietošanu.

3.1.1. Samazināt drošības riskus, ko rada neatbilstoša lietošana, neatļauta piekļuve vai ļaunatūras ieviešana.

3.1.2. Aizsargāt uzņēmuma datus, klientu informāciju un uzņēmuma reputāciju.

3.1.3. Noteikt saistošus noteikumus un nodrošināt atbildību visiem lietotājiem.

3.1.4. Atbalstīt uzraudzību un atbilstību, lai savlaicīgi konstatētu pārkāpumus un īstenotu korektīvas darbības.

4. Lomas un atbildība

4.1. Vispārējais direktors

4.1.1. apstiprina šo politiku un nodrošina, ka tās ieviešanai ir pieejami nepieciešamie resursi un pilnvaras;

4.1.2. pārskata un apstiprina jebkurus izņēmumus no šīs politikas.

4.2. IT vadītājs vai ārējais IT pakalpojumu sniedzējs

4.2.1. uztur apstiprinātās programmatūras un aparatūras uzskaiti;

4.2.2. konfigurē ierīces tā, lai tiktu piemēroti pieļaujamās lietošanas noteikumi, tostarp satura filtrēšana un piekļuves notikumu žurnalēšana;

4.2.3. uzrauga lietošanu, lai identificētu iespējamos pārkāpumus, un izmeklē incidentus;

4.2.4. nodrošina, ka personīgās ierīces (BYOD), ja tās tiek izmantotas uzņēmuma vajadzībām, ir atļautas un drošas.

[... 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 IT vadītājam jāpārskata vismaz reizi gadā, un galīgais apstiprinājums jāsniedz vispārējam direktoram, lai nodrošinātu tās atbilstību tehnoloģiju lietošanas paradumiem, jaunajiem riskiem un atbilstības prasībām.

9.2. Starpposma pārskatīšanas ierosinātāji

9.2.1. Pārskatīšana jāveic arī šādos gadījumos:

9.2.2. tiek ieviestas jaunas sistēmas vai tehnoloģijas, piemēram, jauns mākoņpakalpojums vai galiekārtu platforma;

9.2.3. notiek būtiski politikas pārkāpumi;

9.2.4. tiek atjaunināti tiesību akti vai līguma noteikumi, kas ietekmē IT lietošanu.

9.3. Izmaiņu dokumentēšana

9.3.1. Visi atjauninājumi jāreģistrē versiju žurnālā, kurā norāda:

9.3.1.1. versijas numuru;

9.3.1.2. pārskatīšanas datumu;

9.3.1.3. izmaiņu kopsavilkumu;

9.3.1.4. apstiprinošo amatpersonu.

9.4. Politikas paziņošana

9.4.1. Šīs politikas pārskatītās versijas jādara pieejamas visiem skartajiem lietotājiem. Darbinieki apstiprina saņemšanu un izpratni kā daļu no saviem drošības izpratnes pienākumiem.

10. Saistītās politikas un sasaiste

10.1. Šī politika darbojas kopā ar vairākām citām SME politikām, lai nodrošinātu visaptverošu drošības atbildības tvērumu:

10.1.1. P4S – Piekļuves kontroles politika: nosaka atļautās lietošanas un kontu ierobežojumu tehnisko un procesuālo ieviešanu.

10.1.2. P8S – Informācijas drošības izpratnes un apmācību politika: nodrošina lietotāju apmācību par pieļaujamās lietošanas robežām un ziņošanas pienākumiem.

10.1.3. P9S – Attālinātā darba politika: regulē uzņēmuma sistēmu lietošanu ārpus uzņēmuma telpām vai attālinātā darba vidē.

10.1.4. P17S – Datu aizsardzības un privātuma politika: nosaka personas datu apstrādes noteikumus, kas pārklājas ar pieļaujamās lietošanas uzraudzību un BYOD.

10.1.5. P30S – Incidentu reaģēšanas politika: nosaka kārtību, kā izmeklēt un apstrādāt neatbilstošu lietošanu vai pieļaujamās lietošanas noteikumu pārkāpumus.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. 5.10. punkts — nosaka prasību organizācijām definēt un ieviest informācijas aktīvu pieļaujamo lietošanu.

11.2. ISO/IEC 27002

11.2.1. 5.10. kontroles pasākums — sniedz vadlīnijas par sistēmu pieļaujamo lietošanu, tostarp atļautu un aizliegtu rīcību.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 — attiecas uz sistēmu lietošanas kontroli, tostarp personīgajām ierīcēm.

11.3.2. AC-20 — nosaka prasību autorizēt un uzraudzīt ārējās sistēmas.

11.3.3. AT-2 — uzsver lietotāju apmācību par pieļaujamās lietošanas praksi.

11.4. ES GDPR

11.4.1. 5. panta 1. punkta f) apakšpunkts — nosaka personas datu integritāti un konfidencialitāti, ko var apdraudēt lietotāju neatbilstoša rīcība.

11.4.2. 32. pants — nosaka pienākumu ieviest tehniskos un organizatoriskos pasākumus sistēmu un datu aizsardzībai.

11.5. ES NIS2

11.5.1. 21. panta 2. punkta b) apakšpunkts — nosaka prasību ieviest atbilstošas drošības politikas, tostarp noteikumus par pieļaujamo lietošanu, lai mazinātu kiberdraudus.

11.6. ES DORA

11.6.1. 9. pants — nosaka IKT risku pārvaldības politikas, kas ietver lietošanas kontroles pasākumus un ieviešanas mehānismus.

11.7. COBIT 2019

11.7.1. DSS05 — drošības pakalpojumu pārvaldība: uzsver uz politiku balstītu lietotāju rīcības kontroli.

11.7.2. BAI08 — zināšanu pārvaldība: attiecas uz izpratni par politikas pienākumiem un apmācību par pieļaujamo lietošanu.