					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P34S					Dokumenta nosaukums: **Mobilo ierīču un BYOD 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	Punkti 5.1, 5.2, 6.1, 6.2, 8	Vispārīgās ISPVS un mobilo ierīču/BYOD kontroles prasības
ISO/IEC 27002:2022	Kontroles pasākumi 5.10–5.13	Detalizēti kontroles pasākumi mobilajām ierīcēm, BYOD un attālajai piekļuvei
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Federālās prasības ierīču, datu nesēju un konfigurācijas kontroles pasākumiem
ES GDPR	Panti 5(1)(f)	personas datu un galiekārtu aizsardzība mobilajās platformās
ES NIS2	Pants 21(2)(d)	darbībkritisku ierīču aizsardzība, tostarp BYOD
ES DORA	Panti 9, 10	IKT risks un darbības nepārtrauktība mobilajām galiekārtām
COBIT 2019	APO13, DSS01, DSS05	IT pārvaldības, operāciju un drošības pakalpojumu kontroles pasākumi

1. Mērķis

1.1. Šī politika nosaka obligātās drošības prasības mobilo ierīču, tostarp viedtālruņu, planšetdatoru un klēpjdatoru, izmantošanai, piekļūstot uzņēmuma informācijai, sistēmām vai pakalpojumiem.

1.2. Tā regulē arī personīgo ierīču izmantošanu (BYOD), lai nodrošinātu klientu un uzņēmuma datu aizsardzību neatkarīgi no tā, kam ierīce pieder.

1.3. Politika nodrošina konsekventus drošības pasākumus mobilajai piekļuvei, palīdz sasniegt ISO/IEC 27001 sertifikācijas mērķus un novērš datu zudumu vai kompromitēšanu nozaudētu, nozagtu vai nepareizi izmantotu mobilo galiekārtu dēļ.

1.4. Tā nodrošina, ka MVU vidē bez specializētām IT komandām mobilo ierīču izmantošanai tiek piemēroti gan tehniskie, gan procesuālie kontroles pasākumi, tostarp attālinātā darba vidēs un mākoņpakalpojumos.

2. Piemērošanas joma

2.1. Šī politika attiecas uz visiem darbiniekiem, līgumslēdzējiem, praktikantiem un pakalpojumu sniedzējiem, kuri:

2.1.1. izmanto mobilo ierīci, lai piekļūtu uzņēmuma datiem vai sistēmām, tos apstrādātu vai glabātu;

2.1.2. pieslēdzas uzņēmuma pakalpojumiem, tostarp e-pastam, koplietojamajām mapēm, mākoņlietotnēm vai iekšējām sistēmām, izmantojot VPN.

2.2. Tā aptver:

2.2.1. visas mobilās ierīces: viedtālruņus, planšetdatorus, klēpjdatorus (uzņēmuma izsniegtus vai personīgus BYOD);

2.2.2. visas operētājsistēmas (piemēram, iOS, Android, Windows, macOS);

2.2.3. visas atrašanās vietas (birojs, mājas, attālināts darbs, publiskas vietas).

2.3. Politika ir piemērojama visās darba vidēs, un tā ir jāievēro neatkarīgi no ierīces īpašumtiesībām.

3. Mērķi

3.1. Novērst datu zudumu: nodrošināt, ka mobilo ierīču izmantošana nepakļauj sensitīvus uzņēmuma vai klientu datus nesankcionētai piekļuvei, zādzībai vai neatbilstošai izmantošanai.

3.2. Noteikt skaidrus BYOD noteikumus: noteikt izpildāmus nosacījumus personīgo ierīču izmantošanai darba vajadzībām, nodrošinot tiesiskos un tehniskos drošības pasākumus.

3.3. Atbalstīt regulatīvo atbilstību: izpildīt ISO/IEC 27001, GDPR, NIS2 un citu tiesisko pienākumu prasības, ieviešot piemērojamus mobilo ierīču drošības pasākumus.

3.4. Samazināt operacionālo risku: mazināt darbības traucējumu iespējamību, ko rada mobilo ierīču neatbilstoša izmantošana, kompromitēšana vai atteice.

3.5. Uzturēt klientu uzticēšanos: apliecināt klientiem un partneriem, ka viņu dati saglabā aizsardzību arī tad, ja tiem piekļūst no mobilajām vai personīgajām ierīcēm.

4. Lomas un pienākumi

4.1. Ģenerāldirektors (GM):

4.1.1. nodrošina pārskatatbildību par šo politiku;

4.1.2. apstiprina jebkādu mobilās piekļuves un BYOD izmantošanu piekļuvei uzņēmuma sistēmām;

4.1.3. nodrošina, ka BYOD vienošanās tiek parakstītas, glabātas un uzraudzītas;

4.1.4. pārbauda, vai ārējie IT pakalpojumu sniedzēji ievieš prasītos mobilo ierīču aizsardzības pasākumus.

4.2. Norīkotais personāls vai IT atbalsts:

4.2.1. palīdz ar darba vajadzībām izmantoto mobilo ierīču iestatīšanu, reģistrēšanu un konfigurēšanu;

4.2.2. ievieš ar mobilajām ierīcēm saistītās piekļuves kontroles, lietotņu ierobežojumus un uzraudzības prasības;

4.2.3. nodrošina incidentu reaģēšanas atbalstu attiecībā uz mobilajām ierīcēm (nozaudētām, nozagtām vai kompromitētām ierīcēm).

[... 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. Ģenerāldirektors (GM) pārskata šo politiku vismaz reizi 12 mēnešos.

9.1.2. Pārskatīšanā jāpārbauda nepārtraukta atbilstība ISO/IEC 27001 prasībām, mobilo tehnoloģiju attīstībai un izmaiņām uzņēmuma darbībā.

9.1.3. Atjauninājumos jāņem vērā arī nesenie incidenti, auditu rezultāti vai normatīvā regulējuma izmaiņas (piemēram, GDPR, NIS2, DORA).

9.2. Starpposma pārskatīšanas ierosinātāji

9.2.1. Šī politika nekavējoties jāatjaunina, ja notiek kāds no šiem gadījumiem:

9.2.1.1. būtisks mobilās drošības incidents (piemēram, pārkāpums, kas radies no nozaudētas vai uzlauztas ierīces);

9.2.1.2. atbalstīto platformu vai mobilo ierīču pārvaldības rīku maiņa;

9.2.1.3. tiesiskā vai regulatīvā regulējuma izmaiņas, kas ietekmē personīgo ierīču izmantošanu vai datu aizsardzību;

9.2.1.4. jaunu lietotņu, pakalpojumu vai trešo pušu rīku ieviešana lietošanai mobilajās ierīcēs.

9.3. Izmaiņu dokumentēšana

9.3.1. Visas pārskatīšanas un atjauninājumi jādokumentē, norādot pārskatīšanas datumu, veiktās izmaiņas un GM apstiprinājumu.

9.3.2. Audita vajadzībām jāglabā versiju kontroles vēsture.

9.4. Komunikācija un piekļuve

9.4.1. GM nodrošina, ka visi lietotāji (darbinieki, līgumslēdzēji, trešās puses) ir informēti par izmaiņām.

9.4.2. Atjauninātajām versijām jābūt viegli pieejamām, piemēram, koplietojamajās mapēs vai iekšējās platformās.

10. Saistītās politikas un sasaiste

10.1. Šī politika ir daļa no kopējā MVU informācijas drošības politiku kopuma un jāievieš kopā ar šādām politikām:

10.1.1. P4S – Piekļuves kontroles politika: nosaka prasības drošas piekļuves pārvaldībai sistēmām, tostarp sistēmām, kurām piekļūst, izmantojot mobilās ierīces. Tā nosaka paroļu pārvaldības un sesiju kontroles prasības.

10.1.2. P8S – Informācijas drošības informētības un apmācības politika: nodrošina, ka lietotāji ir apmācīti drošā mobilo ierīču izmantošanā, incidentu ziņošanā un BYOD nosacījumos.

10.1.3. P17S – Datu aizsardzības un privātuma politika: nosaka GDPR prasībām atbilstošu personas datu un uzņēmuma datu apstrādi mobilajās platformās, īpaši, ja darbam tiek izmantotas personīgās ierīces.

10.1.4. P9S – Attālinātā darba politika: ir saskaņota ar mobilo ierīču izmantošanas prasībām darbā ārpus organizācijas telpām vai no mājām, tostarp attiecībā uz ierīču lietošanu un tīkla piekļuves drošības pasākumiem.

10.1.5. P30S – Incidentu reaģēšanas politika: nosaka reaģēšanas ietvaru ar mobilajām ierīcēm saistītiem incidentiem, tostarp kompromitētām vai nozaudētām ierīcēm.

10.2. Šīs saistītās politikas kopā veido pilnīgu kontroles pasākumu kopumu mobilo ierīču drošībai MVU bez specializēta IT personāla, nodrošinot piemērojamību, pārredzamību un gatavību sertifikācijai.

11. Atsauces standarti un ietvari

11.1. Šī politika atbalsta pilnīgu saskaņotību ar šādiem drošības un atbilstības standartiem:

11.2. ISO/IEC 27001:

11.2.1. Punkts 5.1 – Vadība un apņemšanās: nodrošina vadības pārraudzību un pārskatatbildību attiecībā uz mobilo piekļuvi un BYOD;

11.2.2. Punkts 6.1 – Darbības risku novēršanai: nosaka pienākumu izvērtēt un apstrādāt mobilo ierīču drošības riskus;

11.2.3. Punkts 8.1 – Darbības plānošana un kontrole: prasa konsekventas mobilās piekļuves procedūras biznesa datu aizsardzībai.

11.3. ISO/IEC 27002:

11.3.1. Kontroles pasākumi 5.10 (mobilo ierīču izmantošana), 5.11 (attālinātais darbs), 5.12 (attālā piekļuve) un 5.13 (BYOD): sniedz ieviešanas vadlīnijas ierīču risku pārvaldībai maza uzņēmuma kontekstā.

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Piekļuves kontrole mobilajām ierīcēm: nosaka drošības iestatījumu prasības autorizētai mobilo ierīču izmantošanai;

11.4.2. AC-20 – Ārējo sistēmu izmantošana: regulē BYOD un attālās piekļuves riskus;

11.4.3. CM-6 – Konfigurācijas iestatījumi: nosaka drošus noklusējuma un pielāgotos iestatījumus mobilajās platformās;

11.4.4. MP-7 – Datu nesēju izmantošana: nosaka pareizu lietošanu un ierobežojumus mobilajai datu glabāšanai un piekļuvei datiem.

11.5. ES GDPR (2016/679):

11.5.1. Pants 5(1)(f) – Integritāte un konfidencialitāte: prasa datu aizsardzību, nodrošinot atbilstošu personas datu drošību, jo īpaši mobilajās platformās;

11.5.2. Pants 32 – Apstrādes drošība: uzliek pienākumu izmantot atbilstošus tehniskos un organizatoriskos pasākumus, lai aizsargātu datus, kuriem piekļūst vai kurus glabā mobilajās ierīcēs.

11.6. ES NIS2 direktīva (2022/2555):

11.6.1. Pants 21(2)(d) – Ierīču drošības pasākumi: prasa drošības kontroles pasākumus aparatūrai un programmatūrai, ko izmanto piekļuvei kritiskām biznesa sistēmām, tostarp personīgajām ierīcēm.

11.7. ES DORA (2022/2554):

11.7.1. Pants 9 – IKT risku pārvaldības ietvars: prasa aizsargāt mobilās galiekārtas, ko izmanto kritiski svarīgai biznesa saziņai un mākoņpakalpojumiem;

11.7.2. Pants 10 – IKT darbības nepārtrauktība: nosaka pienākumu nodrošināt nepārtrauktu drošu piekļuvi biznesa sistēmām arī traucējumu laikā vai attālināta darba apstākļos.

11.8. COBIT 2019:

11.8.1. APO13 – Pārvaldīt drošību: prasa organizācijai ieviest mobilās lietošanas un BYOD politikas, kas ir saskaņotas ar uzņēmuma riska profilu;

11.8.2. DSS01 – Pārvaldīt operācijas: nodrošina drošas piekļuves mehānismu tehnisko ieviešanu;

11.8.3. DSS05 – Pārvaldīt drošības pakalpojumus: regulē trešo pušu iesaisti drošas mobilās vides uzturēšanā un incidentu reaģēšanas koordinācijā.