					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P34					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 piemērojamajiem standartiem un normatīvajiem aktiem

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Piemēro drošības kontroles un atbilstības prasības
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Nosaka detalizētas kontroles prasības mobilo ierīču pārvaldībai
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Piekļuves kontrole, attālā piekļuve, konfigurācija un drošības prasības mobilajai piekļuvei
ES GDPR	5(1)(f), 25, 32	Obligātas privātuma, datu šifrēšanas un apstrādes drošības prasības
ES NIS2	21(2)(d)	Tehniskie un organizatoriskie aizsardzības pasākumi mobilajai piekļuvei
ES DORA	9, 10	IKT risku pārvaldība un drošības prasības mobilajai piekļuvei
COBIT 2019	APO13.02, DSS01.04, BAI09	Informācijas drošības plāni, aktīvu konfigurācija un kontroles pasākumi mobilajās vidēs

1. Mērķis

1.1 Šī politika nosaka drošības, atbilstības un darbības prasības mobilo ierīču un personīgo tehnoloģiju izmantošanai (BYOD – personīgo ierīču izmantošana), piekļūstot organizācijas sistēmām, lietojumprogrammām vai datiem.

1.2 Tās mērķis ir nodrošināt uzņēmuma informācijas konfidencialitāti, integritāti un pieejamību (CIA), ja tai piekļūst vai tā tiek apstrādāta, izmantojot mobilās galiekārtas, tostarp viedtālruņus, planšetdatorus, klēpjdatorus un hibrīdierīces.

1.3 Tā nosaka arī tehniskās un procesuālās kontroles, kas nepieciešamas, lai mazinātu tādus riskus kā datu noplūde, nesankcionēta piekļuve, ierīces nozaudēšana vai zādzība, kā arī mobilo lietotņu kompromitēšana.

1.4 Šī politika atbalsta normatīvo un līgumisko atbilstību, vienlaikus nodrošinot drošu mobilo darba vidi darbiniekiem, līgumslēdzējiem un autorizētām trešajām pusēm.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visu personālu, tostarp darbiniekiem, līgumslēdzējiem, praktikantiem un trešo pušu pakalpojumu sniedzējiem, kuri izmanto mobilās ierīces, lai piekļūtu uzņēmuma datiem, sistēmām, lietojumprogrammām vai saziņas platformām.

2.2 Tā attiecas uz visām mobilajām skaitļošanas ierīcēm, tostarp, bet ne tikai, uz:

2.2.1 viedtālruņiem un planšetdatoriem (iOS, Android u.c.)

2.2.2 klēpjdatoriem un ultrabook tipa ierīcēm (Windows, macOS, Linux)

2.2.3 valkājamām ierīcēm un hibrīdām viedierīcēm ar datu sinhronizācijas iespējām

2.3 Tā ir piemērojama neatkarīgi no tā, vai ierīce pieder uzņēmumam vai ir personīgā ierīce, kas tiek izmantota saskaņā ar BYOD vienošanos.

2.4 Politika aptver visus piekļuves kanālus, tostarp uzņēmuma VPN, virtuālās darbvirsmas infrastruktūru (VDI), mākoņlietotnes, e-pastu, sadarbības platformas (piemēram, SharePoint, Teams) un failu sinhronizācijas rīkus (piemēram, OneDrive, Dropbox, ja to lietošana ir autorizēta).

2.5 Tā ietver izmantošanu attālinātā darba režīmā, klātienē, komandējumu laikā vai hibrīdā darba organizācijā.

3. Mērķi

3.1 Samazināt datu kompromitēšanas, datu noplūdes vai datu zuduma risku, kas izriet no nedrošas mobilo ierīču lietošanas.

3.2 Nodrošināt konsekventu un izpildāmu drošības kontroļu ieviešanu visās mobilajās galiekārtās neatkarīgi no īpašumtiesību modeļa (uzņēmuma vai BYOD).

3.3 Nodrošināt, ka mobilo ierīču izmantošana atbilst ISO/IEC 27001 un citiem normatīvajiem ietvariem, kas piemērojami datu privātumam, datu aizsardzībai un kiberdrošībai.

3.4 Veicināt drošu mobilo ierīču integrāciju organizācijas darbības, saziņas un sadarbības procesos.

3.5 Nodrošināt skaidri noteiktus pienākumus un procesus mobilo ierīču pārvaldībai (MDM), tostarp ierīču reģistrēšanai, attālinātai datu dzēšanai, šifrēšanai, autentifikācijai un uzraudzībai.

3.6 Aizsargāt to personu privātuma tiesības, kuras izmanto savas ierīces, vienlaikus aizsargājot organizācijas sensitīvos datus.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO) / IT drošības vadītājs

4.1.1 Nosaka politiku un tehniskos standartus mobilo ierīču un BYOD izmantošanai.

4.1.2 Veic atbilstības, incidentu reaģēšanas un izņēmumu pārvaldības uzraudzību attiecībā uz mobilo ierīču kontrolēm.

4.1.3 Koordinē sadarbību ar personālvadības un juridiskā dienesta komandām, lai nodrošinātu, ka politikas piemērošana ir tiesiski pamatota un saskaņota organizācijas ietvarā.

4.2 Informācijas tehnoloģiju (IT) administrators / MDM administrators

4.2.1 Pārvalda mobilo ierīču piekļuves piešķiršanu, reģistrēšanu un konfigurēšanu, izmantojot MDM risinājumus.

4.2.2 Ievieš ierīces līmeņa kontroles pasākumus (piemēram, šifrēšanu, PIN kodus, lietotņu kontroles pasākumus).

4.2.3 Veic attālinātu datu dzēšanu, ierīces bloķēšanu un piekļuves tiesību atsaukšanu, kad tas ir nepieciešams.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā galvenajam informācijas drošības vadītājam (CISO) vai norīkotam informācijas drošības vadītājam, lai nodrošinātu saskaņotību ar:

9.1.1 izmaiņām mobilo operētājsistēmu platformās, MDM tehnoloģijās vai autentifikācijas standartos;

9.1.2 normatīvām vai līgumiskām izmaiņām, kas ietekmē mobilo datu aizsardzību (piemēram, GDPR, DORA, NIS2);

9.1.3 ISO/IEC 27001:2022, ISO/IEC 27002:2022 vai NIST SP 800-53 Rev.5 kontroles pasākumu kopu grozījumiem;

9.1.4 auditu, pēcincidentu izvērtējumu vai darbinieku ziņojumu atgriezenisko saiti.

9.2 Starpposma pārskatīšanu var ierosināt:

9.2.1 drošības incidenti, kuros iesaistītas mobilās ierīces vai BYOD platformas;

9.2.2 piegādātāja paziņojums par augsta riska ievainojamībām atbalstītajās platformās;

9.2.3 jaunu mobilo lietotņu vai sadarbības platformu ieviešana izmantošanai biznesa procesu nodrošināšanā.

9.3 Politikas atjauninājumiem ir jābūt:

9.3.1 dokumentētiem politikas versiju vēsturē;

9.3.2 paziņotiem visam personālam un ietekmētajiem līgumslēdzējiem;

9.3.3 atkārtoti apliecinātiem ar atjauninātu politikas apliecinājumu visiem BYOD lietotājiem.

9.4 Visas pārskatīšanas un redakcijas formāli jāapstiprina izpildvadībai un jāreģistrē politikas grozījumu reģistrā.

10. Saistītās politikas un sasaiste

10.1 Šī politika ir savstarpēji saistīta ar vairākām galvenajām politikām organizācijas IDPS ietvarā. Būtiskākās saiknes ietver:

10.1.1 P1 – Informācijas drošības politika: nosaka vispārējos pārvaldības principus visām informācijas drošības kontrolēm, tostarp tām, kas attiecas uz mobilo ierīču izmantošanu.

10.1.2 P3 – Pieņemamas lietošanas politika: definē pieļaujamo rīcību un ierobežojumus tehnoloģiju izmantošanā, kas tieši attiecas uz mobilo ierīču un BYOD piekļuvi.

10.1.3 P9 – Attālinātā darba politika: nosaka papildu drošības pienākumus mobilā darba vidēm, papildinot šajā politikā noteiktās mobilajām ierīcēm specifiskās kontroles.

10.1.4 P13 – Datu klasifikācijas un marķēšanas politika: nosaka, kā mobilajās ierīcēs esošie dati jāapstrādā atbilstoši klasifikācijas līmenim, ietekmējot glabāšanas, pārsūtīšanas un šifrēšanas prasības.

10.1.5 P22 – Žurnālfiksēšanas un uzraudzības politika: atbalsta mobilās piekļuves žurnālu vākšanu un pārskatīšanu, lai noteiktu anomālijas vai pārkāpumus.

10.1.6 P30 – Incidentu reaģēšanas politika: nosaka, kā tiek apstrādāti un eskalēti ar mobilajām ierīcēm saistīti incidenti (piemēram, ierīces nozaudēšana, nesankcionēta piekļuve).

10.1.7 P33 – Audita un atbilstības uzraudzības politika: nodrošina pamatu periodiskām pārbaudēm attiecībā uz mobilo ierīču drošības atbilstību, tostarp BYOD politikas ievērošanu.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem kiberdrošības ietvariem un tiesiskajiem pienākumiem, lai nodrošinātu drošu mobilo ierīču un personīgo tehnoloģiju (BYOD) izmantošanu uzņēmuma vidē.

11.2 ISO/IEC 27001:

11.2.1 Punkts 5.10 – Pieļaujamā uzņēmuma aktīvu izmantošana: nosaka kontroles pasākumus atbildīgai uzņēmuma aktīvu izmantošanai, tostarp mobilajām ierīcēm.

11.2.2 Punkts 5.11 – Attālinātais darbs: nosaka drošas prakses, piekļūstot sistēmām ārpus uzņēmuma telpām.

11.2.3 Punkts 5.12 – Mobilo ierīču izmantošana: nosaka uz risku balstītas kontroles mobilajām galiekārtām un BYOD konfigurācijām.

11.2.4 Punkts 5.13 – Informācijas pārsūtīšana: nosaka aizsardzības prasības informācijai, kas tiek pārsūtīta, izmantojot mobilos kanālus.

11.3 ISO/IEC 27002:2022 – 5.10 līdz 5.13 kontroles pasākumi:

11.3.1 A pielikuma 5.10 līdz 5.13 kontroles pasākumi: nosaka, kā IDPS ietvarā jāievieš mobilā piekļuve, šifrēšana, uzraudzība un zaudējumu mazināšana. Šie kontroles pasākumi sniedz detalizētas ieviešanas vadlīnijas mobilo galiekārtu aizsardzībai, konteinerizācijas piemērošanai,

ierīču integritātes uzraudzībai un privātumu respektējošu konfigurāciju nodrošināšanai BYOD izmantošanai.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – mobilo ierīču piekļuves kontrole: nosaka pamatlīmeņa aizsardzības pasākumus, tostarp šifrēšanu, autentifikāciju un MDM piemērošanu.

11.4.2 AC-17 – Attālā piekļuve: nosaka drošu autentifikāciju un sesiju aizsardzību attālinātiem mobilo ierīču lietotājiem.

11.4.3 CM-7 – minimālās funkcionalitātes princips: atbalsta nevajadzīgo lietotņu un funkciju noņemšanu no mobilajām galiekārtām riska mazināšanai.

11.4.4 MP-5 – datu nesēju pārvadāšanas aizsardzība: nosaka drošu datu pārsūtīšanu no mobilajām sistēmām uz ārējiem galamērķiem vai mākoņpakalpojumiem.

11.4.5 SC-12 – kriptogrāfisko atslēgu izveide: nosaka drošu kriptogrāfisko protokolu izmantošanu mobilajai saziņai un glabāšanai.

11.5 ES GDPR (2016/679):

11.5.1 Pants 5(1)(f) – integritāte un konfidencialitāte: nosaka pienākumu organizācijām aizsargāt personas datus mobilajās ierīcēs pret nesankcionētu vai nelikumīgu piekļuvi.

11.5.2 Pants 25 – datu aizsardzība pēc projektēšanas un pēc noklusējuma: nosaka prasību iestrādāt privātuma prasības BYOD un MDM procesos.

11.5.3 Pants 32 – apstrādes drošība: nosaka uz risku balstītas kontroles (piemēram, šifrēšanu, autentifikāciju, piekļuves kontroli) personas datiem mobilajās platformās.

11.6 ES NIS2 direktīva (2022/2555):

11.6.1 Pants 21(2)(d): nosaka, ka mobilā piekļuve kritiskām sistēmām un informācijai jāaizsargā ar atbilstošiem tehniskiem un organizatoriskiem pasākumiem, piemēram, galiekārtu kontroli, šifrēšanu un uzraudzību.

11.7 ES DORA (2022/2554):

11.7.1 Pants 9 – IKT risku pārvaldības ietvars: nosaka finanšu sektora subjektiem pienākumu mazināt mobilās un attālās piekļuves riskus kā daļu no darbības noturības.

11.7.2 Pants 10 – IKT sistēmu drošības prasības: nosaka drošu mobilo arhitektūru, uzraudzību un reaģēšanas mehānismus pret kiberdraudiem, kuru izcelsme ir mobilajās ierīcēs.

11.8 COBIT 2019:

11.8.1 APO13.02 – Izveidot un uzturēt informācijas drošības plānu: nosaka, ka mobilo ierīču izmantošana, tostarp BYOD, ir jāintegrē organizācijas drošības stratēģijās.

11.8.2 DSS01.04 – pārvaldīt aktīvu konfigurāciju un integritāti: attiecas uz konfigurācijas kontroli un drošu mobilo ierīču ieviešanu.

11.8.3 BAI09.01 – Izveidot un uzturēt kontroles pasākumus: atbalsta tehnisko un procesuālo drošības pasākumu ieviešanu drošām mobilajām un attālajām operācijām.