					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P34					Názov dokumentu: **Politika mobilných zariadení a používania vlastných zariadení (BYOD)**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Stanovuje bezpečnostné kontroly a požiadavky na súlad
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Poskytuje podrobné kontroly pre riadenie mobilných zariadení
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Riadenie prístupu, vzdialený prístup, konfigurácia a bezpečnostné požiadavky pre mobilné zariadenia
Nariadenie EÚ GDPR	5(1)(f), 25, 32	Záväzné požiadavky na ochranu súkromia, šifrovanie údajov a bezpečnosť spracúvania
Smernica EÚ NIS2	21(2)(d)	Technické a organizačné ochranné opatrenia pre mobilný prístup
Nariadenie EÚ DORA	9, 10	Riadenie IKT rizík a bezpečnostné požiadavky pre mobilné zariadenia
COBIT 2019	APO13.02, DSS01.04, BAI09	Plány informačnej bezpečnosti, konfigurácia aktív a kontroly pre mobilné prostredia

1. Účel

1.1 Táto politika stanovuje bezpečnostné, súladové a prevádzkové požiadavky na používanie mobilných zariadení a osobných technológií v režime používania vlastných zariadení (BYOD) pri prístupe k systémom, aplikáciám alebo údajom organizácie.

1.2 Jej cieľom je zabezpečiť dôvernosť, integritu a dostupnosť informácií organizácie, ku ktorým sa pristupuje alebo ktoré sa spracúvajú prostredníctvom mobilných koncových zariadení vrátane smartfónov, tabletov, notebookov a hybridných zariadení.

1.3 Zároveň zavádza technické a procesné kontroly potrebné na zmiernenie rizík, ako sú únik údajov, neoprávnený prístup, strata alebo krádež zariadenia a kompromitácia mobilných aplikácií.

1.4 Táto politika podporuje plnenie regulačných a zmluvných požiadaviek a zároveň umožňuje bezpečný mobilný výkon pracovných činností zamestnancom, zmluvným pracovníkom a oprávneným tretím stranám.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetok personál vrátane zamestnancov, zmluvných pracovníkov, stážistov a poskytovateľov služieb tretích strán, ktorí používajú mobilné zariadenia na prístup k údajom, systémom, aplikáciám alebo komunikačným platformám organizácie.

2.2 Zahŕňa všetky mobilné výpočtové zariadenia vrátane, ale nielen:

2.2.1 smartfónov a tabletov (iOS, Android a pod.)

2.2.2 notebookov a ultrabookov (Windows, macOS, Linux)

2.2.3 nositeľných zariadení a hybridných inteligentných zariadení schopných synchronizácie údajov

2.3 Uplatňuje sa bez ohľadu na to, či je zariadenie vo vlastníctve organizácie alebo ide o súkromné zariadenie používané na základe dohody BYOD.

2.4 Politika sa vzťahuje na všetky spôsoby prístupu vrátane VPN, virtuálnych desktopov, cloudových aplikácií, e-mailu, platforiem na spoluprácu (napr. SharePoint, Teams) a nástrojov na synchronizáciu súborov (napr. OneDrive, Dropbox, ak sú schválené).

2.5 Zahŕňa používanie pri práci na diaľku, v priestoroch organizácie, počas pracovných ciest alebo v hybridnom režime práce.

3. Ciele

3.1 Znížiť riziko kompromitácie, úniku alebo straty údajov v dôsledku nebezpečného používania mobilných zariadení.

3.2 Uplatňovať konzistentné a vynútiteľné bezpečnostné kontroly na všetkých mobilných koncových zariadeniach bez ohľadu na model vlastníctva (podnikové alebo BYOD).

3.3 Zabezpečiť, aby používanie mobilných zariadení bolo v súlade s ISO/IEC 27001 a ďalšími regulačnými rámcami uplatniteľnými na ochranu súkromia, ochranu údajov a kybernetickú bezpečnosť.

3.4 Umožniť bezpečnú integráciu mobilných zariadení do prevádzkových, komunikačných a kolaboračných pracovných tokov organizácie.

3.5 Poskytnúť jasne definované zodpovednosti a procesy pre správu mobilných zariadení (MDM) vrátane registrácie, vzdialeného vymazania, šifrovania, autentifikácie a monitorovania.

3.6 Chrániť práva na súkromie osôb používajúcich vlastné zariadenia a zároveň chrániť citlivé informácie organizácie.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO) / vedúci informačnej bezpečnosti

4.1.1 Definuje politiku a technické štandardy pre používanie mobilných zariadení a BYOD.

4.1.2 Vykonáva dohľad nad súladom, reakciou na incidenty a riadením výnimiek pre kontroly mobilných zariadení.

4.1.3 Koordinuje postup s právnym oddelením a oddelením ľudských zdrojov s cieľom zabezpečiť, aby uplatňovanie politiky bolo právne obhájiteľné a v súlade s potrebami organizácie.

4.2 IT administrátor / správca MDM

4.2.1 Riadi zriaďovanie, registráciu a konfiguráciu mobilných zariadení prostredníctvom riešení MDM.

4.2.2 Uplatňuje kontroly na úrovni zariadenia (napr. šifrovanie, PIN kódy, kontroly aplikácií).

4.2.3 Vykonáva vzdialené vymazanie, zablokovanie zariadenia a odobratie prístupových oprávnení, ak je to potrebné.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Túto politiku musí najmenej raz ročne preskúmať CISO alebo určený manažér informačnej bezpečnosti, aby sa zabezpečil súlad s:

9.1.1 zmenami platforiem mobilných operačných systémov, technológií MDM alebo autentifikačných štandardov,

9.1.2 regulačnými alebo zmluvnými zmenami ovplyvňujúcimi ochranu mobilných údajov (napr. GDPR, DORA, NIS2),

9.1.3 revíziami súborov kontrol ISO/IEC 27001:2022, ISO/IEC 27002:2022 alebo NIST SP 800-53 Rev.5,

9.1.4 spätnou väzbou z auditov, poincidentných analýz alebo hlásení zamestnancov.

9.2 Mimoriadne preskúmania môžu byť vyvolané:

9.2.1 bezpečnostnými incidentmi zahŕňajúcimi mobilné zariadenia alebo platformy BYOD,

9.2.2 oznámením dodávateľa o vysokorizikových zraniteľnostiach v podporovaných platformách,

9.2.3 zavedením nových mobilných aplikácií alebo platforiem spolupráce používaných na prevádzkové činnosti organizácie.

9.3 Aktualizácie politiky musia byť:

9.3.1 zdokumentované v histórii verzií politiky,

9.3.2 komunikované všetkým zamestnancom a dotknutým zmluvným pracovníkom,

9.3.3 opätovne potvrdené aktualizovaným potvrdením oboznámenia sa pre všetkých používateľov BYOD.

9.4 Všetky preskúmania a revízie musia byť formálne schválené výkonným manažmentom a zaznamenané v registri zmien politík.

10. Súvisiace politiky a väzby

10.1 Táto politika je prepojená s viacerými kľúčovými politikami v rámci systému manažérstva informačnej bezpečnosti organizácie. Medzi najvýznamnejšie väzby patria:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje nadradené princípy správy a riadenia pre všetky kontroly informačnej bezpečnosti vrátane kontrol používania mobilných zariadení.

10.1.2 P3 – Politika prijateľného používania: definuje prípustné správanie a obmedzenia súvisiace s používaním technológií, ktoré sa priamo uplatňujú na mobilný prístup a BYOD.

10.1.3 P9 – Politika práce na diaľku: upravuje dodatočné bezpečnostné povinnosti pre mobilné pracovné prostredia a dopĺňa mobilné kontroly definované v tejto politike.

10.1.4 P13 – Politika klasifikácie a označovania údajov: upravuje, ako sa musí nakladať s údajmi na mobilných zariadeniach podľa úrovne klasifikácie, čo ovplyvňuje uchovávanie, prenos a uplatňovanie šifrovania.

10.1.5 P22 – Politika logovania a monitorovania: podporuje zber a preskúmanie záznamov mobilného prístupu na odhaľovanie anomálií alebo porušení.

10.1.6 P30 – Politika reakcie na incidenty: upravuje spôsob riešenia a eskalácie incidentov súvisiacich s mobilnými zariadeniami (napr. strata zariadenia, neoprávnený prístup).

10.1.7 P33 – Politika monitorovania auditu a súladu: poskytuje základ pre pravidelné kontroly súladu mobilnej bezpečnosti vrátane dodržiavania politiky BYOD.

11. Referenčné normy a rámce

11.1 Táto politika je v súlade s medzinárodne uznávanými rámcami kybernetickej bezpečnosti a právnymi povinnosťami s cieľom zabezpečiť bezpečné používanie mobilných zariadení a osobných technológií v režime BYOD v podnikových prostrediach.

11.2 ISO/IEC 27001:

11.2.1 Bod 5.10 – Prípustné používanie informácií a aktív: vyžaduje kontroly zodpovedného používania podnikových aktív vrátane mobilných zariadení.

11.2.2 Bod 5.11 – Práca na diaľku: upravuje bezpečné postupy pri prístupe k systémom mimo priestorov organizácie.

11.2.3 Bod 5.12 – Používanie mobilných zariadení: vyžaduje kontroly mobilných koncových zariadení a konfigurácií BYOD založené na riziku.

11.2.4 Bod 5.13 – Prenos informácií: uplatňuje ochranu informácií prenášaných prostredníctvom mobilných kanálov.

11.3 ISO/IEC 27002:2022 – Kontroly 5.10 až 5.13:

11.3.1 Kontroly prílohy A 5.10 až 5.13: určujú, ako sa má v rámci ISMS uplatňovať mobilný prístup, šifrovanie, monitorovanie a zmierňovanie strát. Tieto kontroly poskytujú podrobné usmernenia na

implementáciu zabezpečenia mobilných koncových zariadení, uplatňovanie kontajnerizácie, monitorovanie integrity zariadení a zabezpečenie konfigurácií zohľadňujúcich ochranu súkromia pri používaní BYOD.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Riadenie prístupu pre mobilné zariadenia: definuje požiadavky referenčnej bezpečnostnej úrovne vrátane šifrovania, autentifikácie a vynucovania MDM.

11.4.2 AC-17 – Vzdialený prístup: vyžaduje bezpečnú autentifikáciu a ochranu relácií pre používateľov mobilného vzdialeného prístupu.

11.4.3 CM-7 – Zásada minimálnej funkčnosti: podporuje odstránenie nepotrebných aplikácií a funkcií z mobilných koncových zariadení s cieľom znížiť riziko.

11.4.4 MP-5 – Ochrana prenosu médií: upravuje bezpečný prenos údajov z mobilných systémov do externých cieľových prostredí alebo cloudových služieb.

11.4.5 SC-12 – Zriaďovanie kryptografických kľúčov: vyžaduje používanie bezpečných kryptografických protokolov pre mobilnú komunikáciu a uchovávanie údajov.

11.5 Nariadenie EÚ GDPR (2016/679):

11.5.1 Článok 5(1)(f) – Integrita a dôvernosť: vyžaduje, aby organizácie chránili osobné údaje na mobilných zariadeniach pred neoprávneným alebo nezákonným prístupom.

11.5.2 Článok 25 – Ochrana súkromia už od návrhu a štandardne: vyžaduje, aby bola ochrana súkromia zabudovaná do procesov BYOD a MDM.

11.5.3 Článok 32 – Bezpečnosť spracúvania: uplatňuje kontroly založené na riziku (napr. šifrovanie, autentifikácia, riadenie prístupu) pre osobné údaje na mobilných platformách.

11.6 Smernica EÚ NIS2 (2022/2555):

11.6.1 Článok 21(2)(d): vyžaduje, aby bol mobilný prístup ku kritickým systémom a informáciám chránený primeranými technickými a organizačnými opatreniami, ako sú kontroly koncových zariadení, šifrovanie a monitorovanie.

11.7 Nariadenie EÚ DORA (2022/2554):

11.7.1 Článok 9 – Rámec riadenia IKT rizík: vyžaduje, aby subjekty finančného sektora zmierňovali riziká mobilného a vzdialeného prístupu ako súčasť prevádzkovej odolnosti.

11.7.2 Článok 10 – Bezpečnostné požiadavky na systémy IKT: vyžaduje bezpečnú mobilnú architektúru, monitorovanie a mechanizmy reakcie na kybernetické hrozby pochádzajúce z mobilných zariadení.

11.8 COBIT 2019:

11.8.1 APO13.02 – Zaviesť a udržiavať plán informačnej bezpečnosti: vyžaduje, aby používanie mobilných zariadení vrátane BYOD bolo integrované do bezpečnostných stratégií organizácie.

11.8.2 DSS01.04 – Riadiť konfiguráciu a integritu aktív: vzťahuje sa na riadenie konfigurácie a bezpečné nasadenie mobilných zariadení.

11.8.3 BAI09.01 – Zaviesť a udržiavať kontroly: podporuje implementáciu technických a procesných ochranných opatrení pre bezpečné mobilné činnosti a vzdialené operácie.