					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P34S					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	Kapitoly 5.1, 5.2, 6.1, 6.2, 8	Všeobecné požiadavky ISMS a požiadavky na kontroly mobilných zariadení/BYOD
ISO/IEC 27002:2022	Kontroly 5.10 – 5.13	Podrobné kontroly pre mobilné zariadenia/BYOD a vzdialený prístup
NIST SP 800-53 Rev. 5	AC-19, AC-20, CM-6, MP-7	Kontroly zariadení, médií a konfigurácie vo federálnom prostredí
GDPR EÚ	Článok 5(1)(f)	Ochrana osobných údajov a mobilných koncových bodov
NIS2 EÚ	Článok 21(2)(d)	Ochrana kriticky dôležitých zariadení organizácie vrátane BYOD
DORA EÚ	Články 9, 10	Riziká IKT a kontinuita činností pre mobilné koncové body
COBIT 2019	APO13, DSS01, DSS05	Správa a riadenie IT, prevádzka a kontroly bezpečnostných služieb

1. Účel

1.1. Táto politika stanovuje záväzné bezpečnostné požiadavky na používanie mobilných zariadení vrátane smartfónov, tabletov a notebookov pri prístupe k informáciám, systémom alebo službám spoločnosti.

1.2. Zároveň upravuje používanie vlastných zariadení (BYOD) s cieľom zabezpečiť ochranu údajov zákazníkov a informácií organizácie bez ohľadu na vlastníka zariadenia.

1.3. Táto politika zavádza konzistentné ochranné opatrenia pre mobilný prístup, podporuje plnenie cieľov certifikácie podľa ISO/IEC 27001 a predchádza strate údajov alebo kompromitácii spôsobenej stratou, odcudzením alebo zneužitím mobilných koncových bodov.

1.4. Zabezpečuje, aby sa v prostredí MSP bez vyhradených IT tímov uplatňovali pri používaní mobilných zariadení technické aj procesné ochranné opatrenia vrátane práce na diaľku a služieb prevádzkovaných v cloudovom prostredí.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetkých zamestnancov, zmluvných pracovníkov, stážistov a poskytovateľov služieb, ktorí:

2.1.1. používajú mobilné zariadenie na prístup k údajom alebo systémom spoločnosti, na ich spracúvanie alebo uchovávanie,

2.1.2. pripájajú sa k službám spoločnosti vrátane e-mailu, zdieľaných priečinkov, cloudových aplikácií alebo interných systémov prostredníctvom VPN.

2.2. Politika sa vzťahuje na:

2.2.1. všetky mobilné zariadenia: smartfóny, tablety a notebooky (zariadenia vydané spoločnosťou aj súkromné zariadenia v režime BYOD),

2.2.2. všetky operačné systémy (napr. iOS, Android, Windows, macOS),

2.2.3. všetky miesta používania (kancelária, domácnosť, vzdialené pracovisko, verejné priestory).

2.3. Táto politika sa uplatňuje vo všetkých pracovných prostrediach a musí sa vynucovať bez ohľadu na vlastníctvo zariadenia.

3. Ciele

3.1. Predchádzať strate údajov: zabezpečiť, aby používanie mobilných zariadení nevystavovalo citlivé údaje spoločnosti alebo zákazníkov neoprávnenému prístupu, odcudzeniu alebo zneužitiu.

3.2. Stanoviť jasné pravidlá pre používanie vlastných zariadení (BYOD): určiť vynútiteľné podmienky používania súkromných zariadení na pracovné účely pri zachovaní právnych a technických ochranných opatrení.

3.3. Podporovať súlad s požiadavkami: plniť požiadavky podľa ISO/IEC 27001, GDPR, NIS2 a ďalšie zákonné povinnosti prostredníctvom vynútiteľných postupov bezpečnosti mobilných zariadení.

3.4. Minimalizovať prevádzkové riziko: znižovať pravdepodobnosť prevádzkového narušenia spôsobeného zneužitím, kompromitáciou alebo zlyhaním mobilného zariadenia.

3.5. Zachovať dôveru zákazníkov: preukázať zákazníkom a partnerom, že ich údaje zostávajú chránené aj pri prístupe z mobilných alebo súkromných zariadení.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM):

4.1.1. zodpovedá za túto politiku,

4.1.2. schvaľuje všetky prípady mobilného prístupu a BYOD na prístup do systémov spoločnosti,

4.1.3. zabezpečuje, aby dohody o BYOD boli podpísané, uchovávané a priebežne kontrolované,

4.1.4. overuje, že externí poskytovatelia IT služieb uplatňujú požadované ochranné opatrenia pre mobilné zariadenia.

4.2. Určený zamestnanec alebo IT podpora:

4.2.1. poskytuje súčinnosť pri nastavení, registrácii a konfigurácii mobilných zariadení používaných na pracovné účely,

4.2.2. uplatňuje kontroly riadenia prístupu súvisiace s mobilnými zariadeniami, obmedzenia aplikácií a monitorovacie mechanizmy,

4.2.3. podporuje riešenie incidentov týkajúcich sa mobilných zariadení (stratené, odcudzené alebo kompromitované zariadenia).

[... 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. Ročné preskúmanie

9.1.1. Generálny manažér (GM) musí túto politiku preskúmať najmenej raz za 12 mesiacov.

9.1.2. Preskúmanie musí overiť trvalý súlad s požiadavkami ISO/IEC 27001, vývojom mobilných technológií a zmenami v prevádzke organizácie.

9.1.3. Aktualizácie musia zohľadniť aj nedávne incidenty, výsledky auditov alebo regulačný vývoj (napr. GDPR, NIS2, DORA).

9.2. Spúšťacie udalosti pre mimoriadne preskúmanie

9.2.1. Táto politika musí byť bezodkladne aktualizovaná, ak nastane niektorá z nasledujúcich udalostí:

9.2.1.1. významný bezpečnostný incident týkajúci sa mobilných zariadení (napr. porušenie ochrany údajov prostredníctvom strateného alebo napadnutého zariadenia),

9.2.1.2. zmena podporovaných platforiem alebo nástrojov správy mobilných zariadení,

9.2.1.3. právna alebo regulačná zmena ovplyvňujúca používanie súkromných zariadení alebo ochranu údajov,

9.2.1.4. zavedenie nových aplikácií, služieb alebo nástrojov tretích strán používaných na mobilných zariadeniach.

9.3. Dokumentovanie zmien

9.3.1. Všetky preskúmania a aktualizácie musia byť zdokumentované vrátane dátumu preskúmania, vykonaných zmien a schválenia GM.

9.3.2. Na účely auditu sa musí uchovávať história verzií.

9.4. Komunikácia a prístup

9.4.1. GM musí zabezpečiť, aby boli všetci používatelia (zamestnanci, zmluvní pracovníci, tretie strany) informovaní o zmenách.

9.4.2. Aktualizované verzie musia byť jednoducho dostupné, napríklad v zdieľaných priečinkoch alebo na interných platformách.

10. Súvisiace politiky a väzby

10.1. Táto politika je súčasťou celkového súboru politík informačnej bezpečnosti pre MSP a musí sa implementovať spolu s týmito politikami:

10.1.1. P4S – Politika riadenia prístupu: stanovuje požiadavky na riadenie bezpečného prístupu do systémov vrátane systémov prístupných cez mobilné zariadenia. Upravuje hygienu hesiel a riadenie relácií.

10.1.2. P8S – Politika povedomia a školení v oblasti informačnej bezpečnosti: zabezpečuje, aby boli používatelia školení v oblasti bezpečného používania mobilných zariadení, nahlasovania incidentov a podmienok BYOD.

10.1.3. P17S – Politika ochrany údajov a súkromia: stanovuje pravidlá nakladania s osobnými údajmi a údajmi spoločnosti na mobilných platformách v súlade s GDPR, najmä ak sa na prácu používajú súkromné zariadenia.

10.1.4. P9S – Politika práce na diaľku: zosúlaďuje požiadavky na používanie mobilných zariadení pri práci mimo pracoviska alebo z domu vrátane požiadaviek na zaobchádzanie so zariadeniami a ochranné opatrenia sieťového prístupu.

10.1.5. P30S – Politika reakcie na incidenty: poskytuje rámec reakcie na incidenty súvisiace s mobilnými zariadeniami vrátane kompromitovaných alebo stratených zariadení.

10.2. Tieto súvisiace politiky spolu vytvárajú úplný súbor kontrol pre bezpečnosť mobilných zariadení v MSP bez vyhradeného IT personálu a zabezpečujú vynútiteľnosť, transparentnosť a pripravenosť na certifikáciu.

11. Referenčné normy a rámce

11.1. Táto politika podporuje úplný súlad s týmito bezpečnostnými a compliance normami:

11.2. ISO/IEC 27001:

11.2.1. Kapitola 5.1 – Vedenie a záväzok: zabezpečuje dohľad manažmentu a zodpovednosť za mobilný prístup a BYOD.

11.2.2. Kapitola 6.1 – Opatrenia na riešenie rizík: vyžaduje, aby boli riziká bezpečnosti mobilných zariadení posúdené a ošetrené.

11.2.3. Kapitola 8.1 – Prevádzkové plánovanie a riadenie: vyžaduje konzistentné postupy mobilného prístupu na ochranu údajov organizácie.

11.3. ISO/IEC 27002:

11.3.1. Kontroly 5.10 (Používanie mobilných zariadení), 5.11 (Práca na diaľku), 5.12 (Vzdialený prístup) a 5.13 (BYOD): poskytujú usmernenia na implementáciu riadenia rizík zariadení v kontexte malého podniku.

11.4. NIST SP 800-53 Rev. 5:

11.4.1. AC-19 – Riadenie prístupu pre mobilné zariadenia: vyžaduje bezpečnostné nastavenia pre autorizované používanie mobilných zariadení.

11.4.2. AC-20 – Používanie externých systémov: upravuje riziká BYOD a vzdialeného prístupu.

11.4.3. CM-6 – Nastavenia konfigurácie: uplatňuje bezpečné predvolené a prispôsobené nastavenia na mobilných platformách.

11.4.4. MP-7 – Používanie médií: upravuje správne používanie a obmedzenia mobilných úložísk a prístupu k údajom.

11.5. Nariadenie EÚ GDPR (2016/679):

11.5.1. Článok 5(1)(f) – Integrita a dôvernosť: vyžaduje ochranu údajov prostredníctvom primeraného zabezpečenia osobných údajov, najmä na mobilných platformách.

11.5.2. Článok 32 – Bezpečnosť spracúvania: ukladá povinnosť používať primerané technické a organizačné opatrenia na ochranu údajov, ku ktorým sa pristupuje alebo ktoré sú uchovávané na mobilných zariadeniach.

11.6. Smernica EÚ NIS2 (2022/2555):

11.6.1. Článok 21(2)(d) – Opatrenia bezpečnosti zariadení: vyžaduje bezpečnostné kontroly hardvéru a softvéru používaného na prístup ku kritickým systémom organizácie vrátane súkromných zariadení.

11.7. Nariadenie EÚ DORA (2022/2554):

11.7.1. Článok 9 – rámec riadenia rizík IKT: vyžaduje ochranu mobilných koncových bodov používaných na kritickú komunikáciu organizácie a cloudové služby.

11.7.2. Článok 10 – kontinuita činností IKT: vyžaduje zachovanie bezpečného prístupu k systémom organizácie aj počas narušení alebo pri práci na diaľku.

11.8. COBIT 2019:

11.8.1. APO13 – Riadenie bezpečnosti: vyžaduje, aby organizácia uplatňovala politiky pre mobilné zariadenia a BYOD zosúladené s podnikovým rizikom.

11.8.2. DSS01 – Riadenie prevádzky: zabezpečuje technickú implementáciu mechanizmov bezpečného prístupu.

11.8.3. DSS05 – Riadenie bezpečnostných služieb: upravuje zapojenie tretích strán do udržiavania bezpečných mobilných prostredí a koordinácie reakcie na incidenty.