					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P34					Název dokumentu: **Politika mobilních zařízení a používání vlastních zařízení (BYOD)**						
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:						
X	Politika		Standard		Postup		Formulář		Registr		Jiné

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Stanoví bezpečnostní opatření a požadavky na soulad
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Poskytuje podrobná opatření pro správu mobilních zařízení
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Řízení přístupu, vzdálený přístup, konfigurace a bezpečnostní požadavky pro mobilní zařízení
GDPR	5 odst. 1 písm. f), 25, 32	Závazné požadavky na ochranu soukromí, šifrování dat a zabezpečení zpracování
směrnice NIS2	21 odst. 2 písm. d)	Technická a organizační bezpečnostní opatření pro mobilní přístup
nařízení DORA	9, 10	Řízení rizik v oblasti ICT a požadavky na bezpečnost ICT pro mobilní zařízení
COBIT 2019	APO13.02, DSS01.04, BAI09	Plány informační bezpečnosti, konfigurace aktiv a opatření pro mobilní prostředí

1. Účel

1.1 Tato politika stanoví bezpečnostní, provozní a související požadavky na soulad pro používání mobilních zařízení a používání vlastních zařízení (BYOD) při přístupu k systémům, aplikacím nebo datům organizace.

1.2 Jejím cílem je zajistit důvěrnost, integritu a dostupnost informací organizace, k nimž je přistupováno nebo které jsou zpracovávány prostřednictvím mobilních koncových zařízení, včetně chytrých telefonů, tabletů, notebooků a hybridních zařízení.

1.3 Dále stanoví technická a procesní opatření nezbytná ke zmírnění rizik, jako jsou únik dat, neoprávněný přístup, ztráta nebo odcizení zařízení a kompromitace mobilních aplikací.

1.4 Tato politika podporuje soulad s právními předpisy a smluvními požadavky a současně umožňuje bezpečné používání mobilních pracovních prostředků zaměstnanci, smluvními pracovníky a oprávněnými třetími stranami.

2. Rozsah

2.1 Tato politika se vztahuje na veškerý personál, včetně zaměstnanců, smluvních pracovníků, stážistů a poskytovatelů služeb třetích stran, kteří používají mobilní zařízení pro přístup k datům, systémům, aplikacím nebo komunikačním platformám organizace.

2.2 Zahrnuje všechna mobilní výpočetní zařízení, mimo jiné:

2.2.1 chytré telefony a tablety (iOS, Android apod.)

2.2.2 notebooky a ultrabooky (Windows, macOS, Linux)

2.2.3 nositelná zařízení a hybridní chytrá zařízení schopná synchronizace dat

2.3 Vztahuje se bez ohledu na to, zda je zařízení ve vlastnictví organizace, nebo je soukromé a používané na základě dohody o BYOD.

2.4 Politika zahrnuje všechny způsoby přístupu, včetně virtuální privátní sítě (VPN), virtuálních desktopových prostředí, cloudových aplikací, elektronické pošty, platforem pro spolupráci (např. SharePoint, Teams) a nástrojů pro synchronizaci souborů (např. OneDrive, Dropbox, pokud jsou povoleny).

2.5 Zahrnuje používání při práci na dálku, v interním prostředí, na cestách nebo v hybridním režimu práce.

3. Cíle

3.1 Snižovat riziko kompromitace, úniku nebo ztráty dat v důsledku nezabezpečeného používání mobilních zařízení.

3.2 Vynucovat konzistentní a vymahatelná bezpečnostní opatření napříč všemi mobilními koncovými zařízeními bez ohledu na model vlastnictví (firemní nebo BYOD).

3.3 Zajistit, aby používání mobilních zařízení bylo v souladu s ISO/IEC 27001 a dalšími regulačními rámci vztahujícími se k ochraně osobních údajů, ochraně dat a kybernetické bezpečnosti.

3.4 Umožnit bezpečnou integraci mobilních zařízení do provozních, komunikačních a kolaborativních pracovních postupů organizace.

3.5 Stanovit jasné odpovědnosti a procesy pro správu mobilních zařízení (MDM), včetně registrace, vzdáleného vymazání, šifrování, autentizace a monitorování.

3.6 Chránit práva na soukromí osob používajících vlastní zařízení při současném zajištění ochrany citlivých informací organizace.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO) / vedoucí IT bezpečnosti

4.1.1 Stanovuje politiku a technické standardy pro používání mobilních zařízení a BYOD.

4.1.2 Vykonává dohled nad souladem, reakcí na incidenty a správou výjimek v oblasti opatření pro mobilní zařízení.

4.1.3 Koordinuje postup s týmy právního oddělení, compliance a HR tak, aby uplatňování požadavků bylo právně obhajitelné a v souladu s nastavením organizace.

4.2 správce informačních technologií (IT) / správce MDM

4.2.1 Zajišťuje zřizování, registraci a konfiguraci mobilních zařízení prostřednictvím řešení MDM.

4.2.2 Uplatňuje bezpečnostní opatření na úrovni zařízení (např. šifrování, PIN, řízení aplikací).

4.2.3 Provádí vzdálené vymazání, uzamčení zařízení a odebrání přístupu, pokud je to vyžadováno.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být nejméně jednou ročně přezkoumána CISO nebo určeným manažerem informační bezpečnosti, aby byl zajištěn soulad s:

9.1.1 změnami v platformách mobilních operačních systémů, technologiích MDM nebo standardech autentizace

9.1.2 regulačními nebo smluvními změnami ovlivňujícími ochranu mobilních dat (např. GDPR, DORA, NIS2)

9.1.3 změnami v souborech opatření ISO/IEC 27001:2022, ISO/IEC 27002:2022 nebo NIST SP 800-53 Rev.5

9.1.4 zpětnou vazbou z auditů, rozborů po incidentech nebo hlášení zaměstnanců

9.2 Mimořádné přezkumy mohou být zahájeny v důsledku:

9.2.1 bezpečnostních incidentů zahrnujících mobilní zařízení nebo platformy BYOD

9.2.2 oznámení dodavatele o zranitelnostech s vysokým rizikem v podporovaných platformách

9.2.3 zavedení nových mobilních aplikací nebo platforem pro spolupráci používaných pro provozní činnosti

9.3 Aktualizace politiky musí být:

9.3.1 zdokumentovány v historii verzí politiky

9.3.2 sděleny veškerému personálu a dotčeným smluvním pracovníkům

9.3.3 znovu potvrzeny aktualizovaným potvrzením seznámení u všech uživatelů BYOD

9.4 Všechny přezkumy a změny musí být formálně schváleny vrcholovým vedením a zaznamenány v registru změn politik.

10. Související politiky a vazby

10.1 Tato politika je provázána s několika klíčovými politikami v rámci systému řízení bezpečnosti informací (ISMS) organizace. Mezi významné vazby patří:

10.1.1 P1 – Politika informační bezpečnosti: Stanoví zastřešující zásady správy a řízení pro všechna opatření informační bezpečnosti, včetně těch, která upravují používání mobilních zařízení.

10.1.2 P3 – Zásady přípustného užívání: Vymezují přípustné chování a omezení související s používáním technologií, která se přímo vztahují na mobilní přístup a BYOD.

10.1.3 P9 – Politika práce na dálku: Stanoví další bezpečnostní povinnosti pro mobilní pracovní prostředí a doplňuje specifická opatření pro mobilní zařízení stanovená touto politikou.

10.1.4 P13 – Politika klasifikace dat a označování: Stanoví, jak musí být s daty na mobilních zařízeních nakládáno podle úrovně klasifikace, což ovlivňuje ukládání, přenos a vynucování šifrování.

10.1.5 P22 – Politika protokolování a monitorování: Podporuje shromažďování a přezkoumávání protokolů mobilního přístupu za účelem detekce anomálií nebo porušení.

10.1.6 P30 – Politika reakce na incidenty: Stanoví, jak jsou řešeny a eskalovány incidenty související s mobilními zařízeními (např. ztráta zařízení, neoprávněný přístup).

10.1.7 P33 – Politika monitorování auditu a souladu: Poskytuje základ pro pravidelné kontroly souladu zabezpečení mobilních zařízení, včetně dodržování politiky BYOD.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s mezinárodně uznávanými rámci kybernetické bezpečnosti a právními povinnostmi s cílem zajistit bezpečné používání mobilních zařízení a vlastních zařízení (BYOD) v podnikovém prostředí.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 5.10 – Přípustné užívání firemního majetku: Vyžaduje opatření pro odpovědné používání firemního majetku, včetně mobilních zařízení.

11.2.2 Kapitola 5.11 – práce na dálku: Upravuje bezpečné postupy při přístupu k systémům mimo prostory společnosti.

11.2.3 Kapitola 5.12 – používání mobilních zařízení: Nařizuje opatření pro mobilní koncová zařízení a konfigurace BYOD založené na rizicích.

11.2.4 Kapitola 5.13 – přenos informací: Stanoví ochranu informací přenášených prostřednictvím mobilních kanálů.

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

11.3.1 Opatření přílohy A 5.10 až 5.13: Stanoví, jak musí být v rámci ISMS uplatňován mobilní přístup, šifrování, monitorování a zmírňování ztrát. Tato opatření poskytují podrobný implementační návod pro zabezpečení mobilních koncových zařízení, vynucování kontejnerizace, monitorování integrity zařízení a zajištění konfigurací BYOD zohledňujících ochranu soukromí.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – řízení přístupu pro mobilní zařízení: Definuje základní ochranná opatření, včetně šifrování, autentizace a vynucování MDM.

11.4.2 AC-17 – vzdálený přístup: Vyžaduje bezpečnou autentizaci a ochranu relací pro vzdálené mobilní uživatele.

11.4.3 CM-7 – princip minimální funkčnosti: Podporuje odstranění nepotřebných aplikací a funkcí z mobilních koncových zařízení za účelem snížení rizika.

11.4.4 MP-5 – ochrana přenosu médií: Upravuje bezpečný přenos dat z mobilních systémů do externích nebo cloudových cílů.

11.4.5 SC-12 – zřízení kryptografických klíčů: Nařizuje používání bezpečných kryptografických protokolů pro mobilní komunikaci a ukládání dat.

11.5 GDPR (2016/679):

11.5.1 Článek 5 odst. 1 písm. f) – integrita a důvěrnost: Vyžaduje, aby organizace chránily osobní údaje na mobilních zařízeních před neoprávněným nebo protiprávním přístupem.

11.5.2 Článek 25 – ochrana osobních údajů již od návrhu a ve výchozím nastavení: Vyžaduje, aby ochrana soukromí byla začleněna do procesů BYOD a MDM.

11.5.3 Článek 32 – zabezpečení zpracování: Stanoví opatření založená na rizicích (např. šifrování, autentizace, řízení přístupu) pro osobní údaje na mobilních platformách.

11.6 směrnice NIS2 (2022/2555):

11.6.1 Článek 21 odst. 2 písm. d): Vyžaduje, aby mobilní přístup ke kritickým systémům a informacím byl chráněn vhodnými technickými a organizačními opatřeními, jako je správa koncových zařízení, šifrování a monitorování.

11.7 nařízení DORA (2022/2554):

11.7.1 Článek 9 – rámec řízení rizik v oblasti ICT: Vyžaduje, aby subjekty finančního sektoru zmírňovaly rizika mobilního a vzdáleného přístupu jako součást provozní odolnosti.

11.7.2 Článek 10 – požadavky na bezpečnost ICT: Vyžaduje bezpečnou mobilní architekturu, monitorování a mechanismy reakce na kybernetické hrozby pocházející z mobilních zařízení.

11.8 COBIT 2019:

11.8.1 APO13.02 – vytvoření a udržování plánu informační bezpečnosti: Vyžaduje, aby používání mobilních zařízení, včetně BYOD, bylo začleněno do bezpečnostních strategií organizace.

11.8.2 DSS01.04 – řízení konfigurace a integrity aktiv: Vztahuje se na řízení konfigurace a bezpečné nasazení mobilních zařízení.

11.8.3 BAI09.01 – vytvoření a udržování opatření: Podporuje zavedení technických a procesních ochranných opatření pro bezpečný mobilní provoz a vzdálené činnosti.