					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P34S					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	Kapitoly 5.1, 5.2, 6.1, 6.2, 8	Obecné požadavky na ISMS a opatření pro mobilní zařízení, BYOD a vzdálený přístup
ISO/IEC 27002:2022	Opatření 5.10–5.13	Podrobná opatření pro mobilní zařízení, BYOD a vzdálený přístup
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Bezpečnostní opatření pro zařízení, média a řízení konfigurace
GDPR	Článek 5 odst. 1 písm. f)	Ochrana osobních údajů a mobilních koncových zařízení
směrnice NIS2	Článek 21 odst. 2 písm. d)	Ochrana zařízení kritických pro podnikání, včetně BYOD
nařízení DORA	Články 9, 10	Řízení ICT rizik a kontinuita činností pro mobilní koncová zařízení
COBIT 2019	APO13, DSS01, DSS05	Řízení a správa IT, provoz a bezpečnostní služby

1. Účel

1.1. Tato politika stanoví závazné bezpečnostní požadavky pro používání mobilních zařízení, včetně chytrých telefonů, tabletů a notebooků, při přístupu k informacím, systémům nebo službám společnosti.

1.2. Současně upravuje používání soukromých zařízení (BYOD), aby byla zajištěna ochrana zákaznických a podnikových dat bez ohledu na vlastnictví zařízení.

1.3. Tato politika zavádí jednotná ochranná opatření pro mobilní přístup, podporuje plnění cílů certifikace podle ISO/IEC 27001 a předchází ztrátě nebo kompromitaci dat v důsledku ztráty, odcizení nebo nesprávného používání mobilních koncových zařízení.

1.4. Zajišťuje, aby při používání mobilních zařízení v SME bez vyhrazených IT týmů byla uplatňována technická i procesní ochranná opatření, včetně práce na dálku a využívání cloudových služeb.

2. Rozsah

2.1. Tato politika se vztahuje na všechny zaměstnance, smluvní pracovníky, stážisty a poskytovatele služeb, kteří:

2.1.1. používají mobilní zařízení pro přístup k datům nebo systémům společnosti, jejich zpracování nebo ukládání,

2.1.2. připojují se ke službám společnosti, včetně e-mailu, sdílených složek, cloudových aplikací nebo interních systémů prostřednictvím VPN.

2.2. Politika zahrnuje:

2.2.1. všechna mobilní zařízení: chytré telefony, tablety a notebooky (firemní i soukromá v režimu BYOD),

2.2.2. všechny operační systémy (např. iOS, Android, Windows, macOS),

2.2.3. všechna místa používání (kancelář, domov, vzdálené pracoviště, veřejné prostory).

2.3. Tato politika se uplatňuje ve všech pracovních prostředích a musí být vynucována bez ohledu na vlastnictví zařízení.

3. Cíle

3.1. Předcházet ztrátě dat: zajistit, aby používání mobilních zařízení nevystavovalo citlivá data společnosti nebo zákazníků neoprávněnému přístupu, odcizení nebo zneužití.

3.2. Stanovit jasná pravidla pro BYOD: vymezit vymahatelné podmínky pro používání soukromých zařízení pro pracovní účely a zajistit právní i technická ochranná opatření.

3.3. Podporovat soulad s právními předpisy: plnit požadavky podle ISO/IEC 27001, GDPR, směrnice NIS2 a dalších právních povinností prostřednictvím vymahatelných postupů zabezpečení mobilních zařízení.

3.4. Minimalizovat provozní rizika: snížit pravděpodobnost provozního narušení způsobeného nesprávným použitím, kompromitací nebo selháním mobilních zařízení.

3.5. Udržet důvěru zákazníků: prokazovat zákazníkům a partnerům, že jejich data zůstávají chráněna i při přístupu z mobilních nebo soukromých zařízení.

4. Role a odpovědnosti

4.1. Generální ředitel (GM):

4.1.1. odpovídá za tuto politiku,

4.1.2. schvaluje veškeré využívání mobilního přístupu a BYOD k systémům společnosti,

4.1.3. zajišťuje, aby dohody o BYOD byly podepsány, uloženy a monitorovány,

4.1.4. ověřuje, že externí poskytovatelé IT služeb uplatňují požadovaná ochranná opatření pro mobilní zařízení.

4.2. Určení pracovníci nebo IT podpora:

4.2.1. zajišťují podporu při nastavení, registraci a konfiguraci mobilních zařízení používaných pro práci,

4.2.2. uplatňují řízení přístupu související s mobilními zařízeními, omezení aplikací a pravidla monitorování,

4.2.3. podporují řešení incidentů souvisejících s mobilními zařízeními (ztracená, odcizená nebo kompromitovaná zařízení).

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

9. Požadavky na přezkoumávání a aktualizaci

9.1. Roční přezkum

9.1.1. Generální ředitel (GM) musí tuto politiku přezkoumat nejméně jednou za 12 měsíců.

9.1.2. Přezkum musí ověřit trvalý soulad s požadavky ISO/IEC 27001, vývojem mobilních technologií a změnami v obchodních činnostech.

9.1.3. Aktualizace musí rovněž zohlednit nedávné incidenty, výsledky auditů nebo vývoj v právní a regulační oblasti (např. GDPR, směrnice NIS2, nařízení DORA).

9.2. Spouštěcí události pro mimořádný přezkum

9.2.1. Tato politika musí být neprodleně aktualizována, pokud nastane některá z následujících skutečností:

9.2.1.1. závažný bezpečnostní incident související s mobilními zařízeními (např. narušení bezpečnosti prostřednictvím ztraceného nebo napadeného zařízení),

9.2.1.2. změna podporovaných platforem nebo nástrojů pro správu mobilních zařízení,

9.2.1.3. právní nebo regulační změna ovlivňující používání soukromých zařízení nebo ochranu údajů,

9.2.1.4. zavedení nových aplikací, služeb nebo nástrojů třetích stran používaných na mobilních zařízeních.

9.3. Dokumentace změn

9.3.1. Všechny přezkumy a aktualizace musí být zdokumentovány, včetně data přezkumu, provedených změn a schválení GM.

9.3.2. Pro účely auditu musí být uchovávána historie verzí.

9.4. Komunikace a přístup

9.4.1. GM musí zajistit, aby byli všichni uživatelé (zaměstnanci, smluvní pracovníci, třetí strany) informováni o změnách.

9.4.2. Aktualizované verze musí být snadno dostupné, například ve sdílených složkách nebo na interních platformách.

10. Související politiky a vazby

10.1. Tato politika je součástí celkového souboru politik informační bezpečnosti pro SME a musí být uplatňována společně s následujícími politikami:

10.1.1. P4S – Politika řízení přístupu: stanoví požadavky na správu bezpečného přístupu k systémům, včetně systémů přístupných prostřednictvím mobilních zařízení. Uplatňuje zásady bezpečné správy hesel a řízení relací.

10.1.2. P8S – Politika zvyšování povědomí o informační bezpečnosti a školení: zajišťuje, aby byli uživatelé školeni v oblasti bezpečného používání mobilních zařízení, hlášení incidentů a podmínek BYOD.

10.1.3. P17S – Politika ochrany dat a soukromí: stanoví pravidla pro nakládání s osobními a firemními daty na mobilních platformách v souladu s GDPR, zejména při používání soukromých zařízení pro práci.

10.1.4. P9S – Politika práce na dálku: sjednocuje očekávání pro používání mobilních zařízení při práci mimo pracoviště nebo z domova, včetně nakládání se zařízeními a ochranných opatření pro přístup k síti.

10.1.5. P30S – Politika reakce na incidenty: poskytuje rámec pro reakci na incidenty související s mobilními zařízeními, včetně kompromitovaných nebo ztracených zařízení.

10.2. Tyto související politiky společně tvoří úplný soubor opatření pro zabezpečení mobilních zařízení v SME bez vyhrazeného IT personálu a zajišťují vymahatelnost, transparentnost a připravenost na certifikaci.

11. Referenční normy a rámce

11.1. Tato politika podporuje plný soulad s následujícími bezpečnostními normami a požadavky na compliance:

11.2. ISO/IEC 27001:

11.2.1. Kapitola 5.1 – Leadership and Commitment: zajišťuje dohled vedení a odpovědnost za mobilní přístup a BYOD,

11.2.2. Kapitola 6.1 – Actions to Address Risks: vyžaduje posouzení a ošetření rizik souvisejících se zabezpečením mobilních zařízení,

11.2.3. Kapitola 8.1 – Provozní plánování a řízení: vyžaduje jednotné postupy mobilního přístupu k ochraně podnikových dat.

11.3. ISO/IEC 27002:

11.3.1. Opatření 5.10 (Use of Mobile Devices), 5.11 (Teleworking), 5.12 (Remote Access) a 5.13 (BYOD): poskytují vodítka pro implementaci řízení rizik zařízení v kontextu malého podniku.

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Access Control for Mobile Devices: vyžaduje bezpečnostní nastavení pro autorizované používání mobilních zařízení,

11.4.2. AC-20 – Use of External Systems: upravuje rizika BYOD a vzdáleného přístupu,

11.4.3. CM-6 – Configuration Settings: uplatňuje bezpečné výchozí i přizpůsobené nastavení na mobilních platformách,

11.4.4. MP-7 – Media Use: řeší správné používání a omezení pro mobilní úložiště a přístup k datům.

11.5. GDPR (EU) 2016/679:

11.5.1. Článek 5 odst. 1 písm. f) – Integrita a důvěrnost: vyžaduje ochranu dat prostřednictvím odpovídajícího zabezpečení osobních údajů, zejména na mobilních platformách,

11.5.2. Článek 32 – Zabezpečení zpracování: ukládá použití vhodných technických a organizačních opatření (TOM) k zabezpečení dat, k nimž je přistupováno nebo která jsou ukládána na mobilních zařízeních.

11.6. směrnice NIS2 (EU) 2022/2555:

11.6.1. Článek 21 odst. 2 písm. d) – opatření k zabezpečení zařízení: vyžaduje bezpečnostní opatření pro hardware a software používaný pro přístup ke kritickým podnikovým systémům, včetně soukromých zařízení.

11.7. nařízení DORA (EU) 2022/2554:

11.7.1. Článek 9 – rámec řízení ICT rizik: vyžaduje ochranu mobilních koncových zařízení používaných pro kritickou podnikovou komunikaci a cloudové služby,

11.7.2. Článek 10 – kontinuita činností v oblasti ICT: vyžaduje zachování bezpečného přístupu k podnikovým systémům i během narušení nebo práce na dálku.

11.8. COBIT 2019:

11.8.1. APO13 – Manage Security: vyžaduje, aby organizace uplatňovala politiky pro mobilní zařízení a BYOD v souladu s podnikovými riziky,

11.8.2. DSS01 – Manage Operations: zajišťuje technickou implementaci mechanismů bezpečného přístupu,

11.8.3. DSS05 – Manage Security Services: upravuje zapojení třetích stran do udržování bezpečného prostředí mobilních zařízení a koordinace reakce na incidenty.