Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-012**
Název dokumentu:	**Politika bezpečného používání mobilních zařízení**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Politika se vztahuje z pohledu organizační struktury VVŠ na jednotlivá oddělení JU, dále pak také na uživatele mobilních zařízení v majetku VVŠ, rovněž na mobilní zařízení v osobním vlastnictví uživatelů uvnitř i vně perimetru VVŠ.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 12, 19, 21, 23
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	2 + 0
Verze:	1.1
Význam a benefity:	Tato politika popisuje jednotlivá pravidla a postupy, která jsou vyžadována pro bezpečné používání mobilních zařízení, z důvodu zvýšeného rizika hrozeb vyplývajících z mobility zařízení.
Uložení:	Sekce kyberbezpečnosti na Wiki JU
Ruší dokumenty:	-
Zpracovatel:	Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

JU musí řídit přístup uživatelů z mobilních zařízení ke svým aktivům, zejména z mobilních telefonů, tabletů a notebooků uživatelů. Do toho spadají i soukromé mobilní zařízení používaná pro pracovní účely.

Uživatelé zároveň musí být dostatečně proškoleni, jak postupovat v případě výskytu bezpečnostních incidentů a měli by před vydáním mobilního zařízení prokázat, že jsou si vědomi možných rizik a nápravných postupů.

a) Pravidla a postupy pro bezpečné používání mobilních zařízení

JU u spravovaných mobilních zařízení:

- zavede zásady bezpečného konfigurování a používání zařízení, které jsou vhodné pro účel zařízení;
- vyžaduje používání bezpečnostních SW (antivir atp.);
- v souladu s Politikou bezpečnosti lidských zdrojů zabezpečí školení a osvětové aktivity pro uživatele mobilních zařízení o hrozbách a doporučených bezpečnostních postupech.

b) Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě

Mobilní zařízení uživatelů, která nejsou centrálně spravována nebo která nesplňují nastavené centrální politiky, nemají stejná práva přístupu ke službám a datům JU, jako zařízení spravovaná.

V odůvodněných případech, za splnění specifických podmínek, může těmto zařízením, na která se ukládají data JU, nebo která k těmto datům vzdáleně přistupují a nespravují je IT specialisté JU, být přístup dočasně i opakovaně umožněn bez ohledu na to, kdo je jejich vlastníkem. Může jít o povinnost zaměstnance předložit (např. každých 14 dní) zařízení ke kontrole IT specialistovi atp.

Zaměstnanec má povinnost zajistit ochranu svého mobilního zařízení.

Evidenci zařízení JU a plnění stanovených podmínek vede a určuje zodpovědná osoba na JU.

1. Použití nedůvěryhodných sítí

Nastavení bezpečného šifrovaného připojení Wi-Fi a VPN musí být součástí základní konfigurace zabezpečení.

2. Použití nedůvěryhodných aplikací

Na mobilní zařízení se nesmí instalovat aplikace třetích stran z nedůvěryhodných zdrojů. Nainstalovaným aplikacím se smí udělit pouze nezbytná oprávnění.

3. Použití nedůvěryhodného obsahu

Uživatelé musí být poučeni o rizicích spojených s nedůvěryhodným obsahem a odradit je od přístupu k nedůvěryhodnému obsahu prostřednictvím mobilních zařízení, která používají k práci. Příkladem jsou QR kódy. Ty jsou speciálně navrženy tak, aby je

zobrazovaly a zpracovávaly kamery mobilních zařízení. Každý kód QR je převeden na text, obvykle adresu URL, takže škodlivé QR kódy mohou mobilní zařízení nasměrovat na škodlivé webové stránky.[1]

Pokud možno, čtečky QR kódů musí být nakonfigurované tak, aby po naskenování kódu zobrazili adresu URL.

4. Fyzické zabezpečení mobilních zařízení

Zaměstnanec, který používá mobilní zařízení mimo perimetru JU, musí důrazně dbát na fyzické zabezpečení těchto mobilních zařízení.

Mobilní zařízení musí být:

- bezpečně uzamčena (za bezpečné uzamčení se nepovažuje např. auto), v případě, že se vyskytují bez dozoru uživatele;
- opatřena bezpečnostními zámky pro různé oblasti dat;
- zašifrována, pokud obsahují citlivé a jinak významné informace, a to nejen o JU.

Zařízení se musí automaticky zamykat po určitém intervalu neaktivity, např. po pěti minutách.

Mobilní telefony a tablety, které obsahují data zaměstnavatele (poštu, kalendář, soubory atd.) musí být chráněny zámkem obrazovky (PIN, gesto, otisk prstu, rozpoznání obličeje).

Historie revizí

Historie revizí je uvedena u souboru této politiky na Wiki JU.

[1] Zdroj: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf