SLEZSKÉ ZEMSKÉ MUZEUM

Směrnice ředitele č. 5/2023

Kybernetická bezpečnost

OBSAH

	Titul, jméno, příjmení	Pracovní zařazení	Podpis
Zpracovatelé	Ing. Petr Kašpar	Vedoucí OPI	
	Simona Čarnecká	Investiční referent	
	Monika Grueberová	Závěrečná redakce směrnice	
Kontrola věcné správnosti	Ing. Tomáš Bartoš	Interní auditor	

Za udržování směrnice v aktuálním stavu zodpovídá		vedoucí OPI	
Účinnost od	24. 7. 2023	Číslo jednací	SZM/001177/2023/OPI
Touto směrnicí se ruší		JID	SZMOSS00272857

Kybernetická bezpečnost

1. Úvod

Směrnice o kybernetické bezpečnosti SZM vychází ze zásad stanovených zákonem o kybernetické bezpečnosti 181/2014 Sb. a návaznými předpisy a z principů směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Evropské unii (NIS2) v platném znění. Cílem směrnice je předcházet kybernetickým útokům a únikům informací prostřednictvím preventivních opatření.

2. Přihlašování a hesla

Hesla pro přístup do webových rozhraní SZM (email, program evidence sbírek, docházkový systém atd.) musí být vybírána tak, aby neobsahovala jméno či příjmení zaměstnance, jeho rok narození či jiné běžně zjistitelné údaje o daném uživateli. Hesla také nesmí být odvozena od názvu či adresy příslušného pracoviště. Doporučuje se užívání hesel, kombinujících písmena, číslice a speciální znaky, a to v délce nejméně 10 znaků. Lze používat tzv. frázová hesla. Zakazuje se ukládání hesel do paměti webových prohlížečů. Lze používat zabezpečené programy pro správu hesel dle doporučení správce informačních a komunikačních technologií SZM či jím pověřené osoby. Po dokončení práce v příslušném webovém rozhraní SZM se zaměstnanec musí vždy odhlásit.

3. Zabezpečení mobilních zařízení

Zaměstnanci jsou povinni dbát bezpečnostních standardů při práci s mobilními zařízeními SZM i s osobními mobilními telefony využívajícími služební SIM karty. Uvedená zařízení musí být zabezpečena kódem PIN a/nebo kontrolním gestem pro odemčení. Kód PIN nesmí být složen z po sobě jdoucích čísel ani vycházet z data narození zaměstnance.

4. Zásady bezpečného připojení

Jelikož povaha výzkumné práce v SZM vyžaduje častý pohyb odborných pracovníků v terénu, lze těmto pracovníkům umožnit vzdálené připojení k webovým rozhraním organizace. Připojení se však musí dít pouze prostřednictvím nástrojů schválených správcem informačních a komunikačních technologií SZM (např. síť VPN). Po dokončení práce je zaměstnanec povinen se z příslušného rozhraní odhlásit. Při připojení k internetovým sítím externích poskytovatelů se doporučuje využití anonymního režimu.

5. Ochrana proti sociálnímu inženýrství

Zaměstnanci nesmí otvírat podezřelé emailové a SMS zprávy, stejně jako zprávy na sociálních sítích. Jedná se především o zprávy neznámých původců, zprávy tvářící se jako reklamní sdělení, vyžadující zadání přihlašovacích údajů či kliknutí na odkaz, zprávy vytvořené prostřednictvím překladače, zprávy žádající o provedení internetové platby apod. Taktéž je zakázáno v telefonátech osobám a institucím mimo SZM sdělovat přihlašovací či citlivé údaje. Jde zejména o telefonáty prezentující se jako nabídky služeb či průzkumy veřejného mínění. Na opakovaný výskyt podezřelých zpráv nebo telefonátů od jednoho původce je zaměstnanec povinen upozornit správce informačních a komunikačních technologií SZM či Krizový štáb SZM.

6. Ochrana proti virům

V rámci ochrany proti virům zaměstnanci nesmí stahovat do počítačů a mobilních zařízení soubory z neznámých zdrojů. Instalaci softwaru provádí pouze správce informačních a komunikačních technologií SZM nebo jím pověřená osoba. Správce informačních a komunikačních technologií také zajišťuje, aby počítače a mobilní zařízení SZM byla chráněna antivirovými programy splňujícími aktuální bezpečnostní standardy. Je zakázáno připojovat k počítačům a mobilním zařízením externí zařízení (flash disk, externí disk, CD, DVD apod.) neznámého původu. Pro předávání souborů osobám a organizacím mimo SZM se doporučuje preferovat online přenos před využíváním flash disků a jiných přenosových zařízení. Zjištěné napadení počítače či mobilního zařízení virem je nutno neprodleně ohlásit správci informačních a komunikačních technologií SZM a přístroj až do provedení kontroly správcem informačních a komunikačních technologií SZM dále nepoužívat.

7. Další preventivní opatření

S ohledem na vývoj kybernetických technologií je nutno průběžně aktualizovat bezpečnostní opatření. Krizový štáb a správce informačních a komunikačních technologií SZM pravidelně kontrolují stav výpočetní techniky a softwaru v organizaci a vyhodnocují potenciální rizika. Správce informačních a komunikačních technologií také zajišťuje průběžnou kontrolu dodržování výše uvedených opatření a dle potřeby zajišťuje informovanost zaměstnanců o nových či aktuálních podobách kybernetických hrozeb.

8. Závěrečné ustanovení

Tato směrnice nabývá účinnosti a platnosti dnem 24. 7. 2023

V Opavě dne 24. 7. 2023

Mgr. Jana Horáková
ředitelka