					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P38					Název dokumentu: **Politika bezpečné komunikace a vícefaktorového ověřování**						
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	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
GDPR	čl. 32 odst. 1 písm. b)	
směrnice NIS2	čl. 21 odst. 2 písm. j)	
nařízení DORA	čl. 9 odst. 2 písm. d), čl. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Účel

1.1 Stanovit požadavky na používání vícefaktorového ověřování (MFA) nebo řešení průběžného ověřování pro přístup do systémů v souladu s čl. 21 odst. 2 písm. j) směrnice NIS2.

1.2 Zavést opatření pro zabezpečenou hlasovou, obrazovou, textovou a nouzovou komunikaci za účelem ochrany důvěrnosti a integrity informací.

2. Rozsah

2.1 Tato politika se vztahuje na všechny mechanismy ověřování a komunikační systémy (hlasové hovory, videokonference, zasílání zpráv a systémy nouzového oznamování) používané organizací.

2.2 Vztahuje se na všechny zaměstnance a smluvní pracovníky i na všechny externí strany využívající komunikační kanály organizace nebo přistupující k jejím síťovým a informačním systémům.

3. Cíle

3.1 Zajistit, aby přístup do systémů získali pouze řádně ověření uživatelé, a snížit tak riziko neoprávněného přístupu prostřednictvím zavedení vícefaktorového ověřování (MFA).

3.2 Zajistit, aby interní i nouzová komunikace byla přenášena zabezpečenými metodami (např. šifrovanými komunikačními kanály), a zabránit tak odposlechu nebo neoprávněné manipulaci.

3.3 Plnit požadavky směrnice NIS2 na silné ověřování a bezpečnou komunikaci, a tím posilovat celkovou kybernetickou odolnost.

4. Role a odpovědnosti

4.1 Ředitel informační bezpečnosti (CISO) / IT bezpečnost: Definuje a udržuje mechanismy MFA a nástroje bezpečné komunikace; zajišťuje technické vynucování této politiky.

4.2 IT administrátoři: Implementují MFA pro relevantní systémy a konfigurují schválené platformy bezpečné komunikace; provádějí monitorování souladu.

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

9. Monitorování a audit

9.1 IT bezpečnost musí průběžně monitorovat protokoly ověřování z hlediska pokusů o přihlášení pouze jedním faktorem nebo anomálních selhání MFA. Protokoly systémů bezpečné komunikace (tam, kde jsou k dispozici) musí být monitorovány z hlediska pokusů o neoprávněný přístup nebo změn konfigurace.

9.2 Interní audit každoročně přezkoumá dodržování implementace MFA (ověří, že všechny kritické systémy MFA vynucují) a ověří, že pro citlivou komunikaci jsou výhradně používány schválené zabezpečené kanály. Zjištění budou oznámena vedení spolu s doporučeními.

10. Přezkum a údržba

10.1 Tato politika bude přezkoumávána nejméně jednou ročně a po každém závažném bezpečnostním incidentu nebo nově identifikovaném riziku souvisejícím s ověřováním nebo komunikací (např. nové vektory hrozeb proti MFA, zjištění používání nezabezpečené komunikace).

10.2 Aktualizace budou prováděny podle potřeby s ohledem na vývoj technologií (např. zavedení robustnějších řešení průběžného ověřování) nebo za účelem souladu s aktualizovanými regulačními doporučeními (např. budoucí doporučení ENISA k bezpečné komunikaci).

11. Související politiky a vazby

11.1 P01 – P01 Politika informační bezpečnosti. Stanoví požadavky na ochranná opatření pro ověřování a komunikaci v celé organizaci.

11.2 P04 – Politika řízení přístupu. Stanoví správu přístupu, kterou MFA podle P38 vynucuje.

11.3 P11 – Politika správy uživatelských účtů a oprávnění. Propojuje MFA se životním cyklem privilegovaného přístupu.

11.4 P18 – Politika kryptografických opatření. Stanoví schválené kryptografické metody a správu klíčů pro bezpečnou komunikaci.

11.5 P21 – Politika zabezpečení sítí. Zabezpečuje přenosové kanály používané pro hlas, obraz a zasílání zpráv.

11.6 P22 – Politika protokolování a monitorování. Zajišťuje monitorování událostí ověřování a používání zabezpečených kanálů.

11.7 P32 – Politika kontinuity činností a obnovy po havárii. Zabezpečuje nouzovou komunikaci během krizových situací.

11.8 P08 – Politika povědomí o informační bezpečnosti a školení. Školí uživatele v oblasti MFA a bezpečné hygieny komunikačních kanálů.

12. Reference

12.1 Směrnice NIS2 (EU 2022/2555), čl. 21 odst. 2 písm. j) (používání vícefaktorového ověřování a zabezpečené komunikace)

12.2 Prováděcí nařízení Komise (EU) 2024/2690, příloha oddíl 11 (požadavky na řízení přístupu, včetně MFA pro privilegované účty)

12.3 ISO/IEC 27001:2022 a ISO/IEC 27002: