					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P19S					Název dokumentu: **Politika řízení zranitelností a záplat**							
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	Ustanovení/článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	
ISO/IEC 27002:2022	Opatření 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
směrnice NIS2	Články 21(2)(d), 21(2)(e)	
nařízení DORA	Články 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
GDPR	Článek 32(1)(b)	

1. Účel

1.1 Tato politika stanoví, jak organizace identifikuje, vyhodnocuje a zmírňuje zranitelnosti v systémech, aplikacích a infrastruktuře.

1.2 Jejím účelem je snižovat kybernetická rizika prostřednictvím včasného záplatování a postupů nápravy založených na riziku, které odpovídají potřebám malých a středních podniků (SME).

1.3 Tato politika podporuje soulad s požadavky na certifikaci podle ISO/IEC 27001:2022 a napomáhá plnění regulačních povinností podle GDPR, směrnice NIS2 a nařízení DORA tím, že vyžaduje proaktivní řízení technických zranitelností.

1.4 Organizace uznává, že nezáplatované systémy představují významné ohrožení bezpečnosti informací a musí být řešeny systematicky a bez zbytečného odkladu.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny servery, stolní počítače, notebooky, mobilní zařízení, síťová zařízení a cloudové platformy používané organizací,

2.1.2 všechny operační systémy, software třetích stran, zásuvné moduly a aplikace používané v rámci podnikových činností,

2.1.3 interní pracovníky IT nebo externí poskytovatele IT služeb odpovědné za údržbu systémů, aktualizace nebo monitorování,

2.1.4 veškerý interně vyvíjený kód nebo vestavěný software spravovaný organizací nebo jejím jménem.

2.2 Politika se vztahuje jak na infrastrukturu spravovanou přímo organizací, tak na systémy spravované smluvními dodavateli nebo poskytovateli hostingu.

3. Cíle

3.1 Včas a konzistentně identifikovat a posuzovat známé zranitelnosti napříč všemi IT aktivy.

3.2 Uplatňovat záplaty a aktualizace softwaru podle závažnosti a rizika pro provoz organizace nebo osobní údaje.

3.3 Předcházet zneužití technických slabin, které by mohly vést k nedostupnosti služeb, narušení bezpečnosti dat nebo nesouladu s právními požadavky.

3.4 Vést přesné záznamy o aplikovaných záplatách, nevyřešených problémech a výjimkách pro účely připravenosti na audit.

3.5 Používat nástroje a procesy odpovídající velikosti organizace a provozní složitosti bez snížení jejich účinnosti.

3.6 Podporovat právní a regulační soulad, včetně článku 32 GDPR a opatření 8 přílohy A normy ISO.

4. Role a odpovědnosti

4.1 generální ředitel

4.1.1 Nese celkovou odpovědnost za zajištění provádění záplatování a řízení zranitelností.

4.1.2 Schvaluje výjimky z akceptace rizik v případech, kdy nelze záplaty aplikovat, a přezkoumává související strategie zmírnění rizik.

4.1.3 Přezkoumává zprávy o stavu záplatování a zajišťuje dostupnost zdrojů potřebných ke splnění povinností v oblasti záplatování.

4.2 poskytovatel IT podpory / interní správce IT

4.2.1 Monitoruje systémy z hlediska zranitelností a dostupných záplat s využitím upozornění dodavatelů, zpravodajství o hrozbách a oznámení na úrovni operačního systému.

4.2.2 Aplikuje aktualizace operačního systému, firmwaru a aplikací ve stanovených lhůtách.

4.2.3 Vede formální evidenci záplat a dokumentuje nevyřešené nebo odložené aktualizace.

4.2.4 Provádí testování a plánování kritických aktualizací s cílem minimalizovat provozní narušení.

[... 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 Tato politika musí být nejméně jednou ročně přezkoumána generálním ředitelem za účasti poskytovatele IT a koordinátora ochrany soukromí.

9.2 Podněty k přezkumu

9.2.1 Mimořádné přezkumy musí proběhnout, pokud:

9.2.1.1 závažná zranitelnost nebo exploit ovlivní systémy v rozsahu této politiky,

9.2.1.2 dojde k významným změnám systémů nebo softwaru,

9.2.1.3 audit identifikuje nedostatky v procesech záplatování,

9.2.1.4 je zaznamenán incident nebo narušení bezpečnosti související se záplatováním.

9.3 Řízení verzí politiky

9.3.1 Všechny aktualizace musí být zaznamenány v evidenci verzí včetně shrnutí změn.

9.3.2 Změny musí být oznámeny dotčenému personálu.

9.3.3 Zastaralé verze musí být archivovány s omezeným přístupem.

10. Související politiky a vazby

10.1 Tato politika podporuje několik dalších SME politik a je na nich závislá:

10.1.1 P12S – Politika správy aktiv: Identifikuje vlastnictví a klasifikaci systémů a zajišťuje, aby všechna aktiva vyžadující záplatování byla zachycena v evidenci aktiv.

10.1.2 P14S – Politika uchovávání údajů: Zajišťuje, aby systémy plánované k vyřazení z provozu byly bezpečně aktualizovány nebo vymazány, čímž se snižuje expozice zranitelnostem.

10.1.3 P17S – Politika ochrany dat a soukromí: Upřednostňuje nápravu zranitelností u systémů zpracovávajících osobní údaje za účelem souladu s právními předpisy v oblasti ochrany soukromí.

10.1.4 P22S – Politika protokolování a monitorování: Podporuje identifikaci nezáplatovaných systémů nebo podezřelého chování, které může signalizovat zneužití zranitelnosti.

10.1.5 P30S – Politika reakce na incidenty: Definuje postupy pro reakci na zranitelnosti, které vedou k bezpečnostním incidentům, včetně eskalace a oznamovacích kroků.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje implementaci opatření k řešení provozních rizik, včetně řízení zranitelností.

11.2 ISO/IEC 27002

11.2.1 Opatření 8.8 – Stanoví procesy pro skenování a odstraňování známých slabin v systémech.

11.2.2 Opatření 8.9 – Zdůrazňuje bezpečnou konfiguraci, ověřování záplat a řízení změn, aby se při aktualizacích předešlo nové expozici.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Vyžaduje identifikaci zranitelností a jejich nápravu ve stanovených lhůtách.

11.3.2 SI-2 – Ukládá neprodlenou aplikaci záplat a aktualizací podle jejich závažnosti.

11.3.3 CM-2 – Upravuje výchozí konfigurace systémů a dokumentaci aktualizací za účelem zajištění konzistentní ochrany.

11.4 GDPR

11.4.1 Článek 32(1)(b) – Vyžaduje, aby organizace zavedly vhodná technická opatření, včetně záplatování, k zajištění bezpečnosti zpracování.

11.5 směrnice NIS2

11.5.1 Článek 21(2)(d) – Vyžaduje řízení zranitelností prostřednictvím systematického skenování a nápravy.

11.5.2 Článek 21(2)(e) – Ukládá bezpečnou konfiguraci a řízení záplat za účelem zajištění odolnosti ICT.

11.6 nařízení DORA

11.6.1 Článek 8(1) – Vyžaduje identifikaci a zmírňování rizik v oblasti ICT, včetně technických zranitelností.

11.6.2 Článek 10(2) – Ukládá finančním subjektům odstraňovat slabiny ovlivňující systémy a provoz v oblasti ICT.

11.7 COBIT 2019

11.7.1 DSS05.02 – Vyžaduje ošetření známých technických zranitelností za účelem zachování bezpečného provozu.

11.7.2 APO12.01 – Propojuje řízení rizik s proaktivním monitorováním a odstraňováním systémových slabin.