					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P24S					Název dokumentu: **Politika bezpečného vývoje**							
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	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Článek 8	Relevantní bezpečnostní opatření pro provozní postupy, včetně bezpečného vývoje
ISO/IEC 27002:2022	Opatření 8.25–8.27	Pokrývá životní cyklus bezpečného vývoje, testování a bezpečnostní odpovědnosti externích vývojářů
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Řeší bezpečný SDLC, řízení přístupu a řešení zranitelností ve vývoji
GDPR	Článek 25	Vyžaduje ochranu osobních údajů již od návrhu a ve výchozím nastavení při vývoji softwaru
směrnice NIS2	Článek 21 odst. 2 písm. a), e), h)	Ukládá povinnost zavést politiky bezpečného vývoje, dohled nad využitím open-source a dokumentaci zmírňujících opatření
nařízení DORA	Články 6 odst. 7, 9 odst. 1 písm. c), 10 odst. 2 písm. c)	Bezpečnost životního cyklu u kritických ICT systémů ve finančním sektoru
COBIT 2019	BAI	Rámec pro strukturované, dohledatelné a odolné řízení bezpečného vývoje

1. Účel

1.1 Tato politika zajišťuje, aby veškerý software, skripty a webové nástroje vytvořené nebo upravené organizací nebo jejími externími partnery byly vyvíjeny bezpečně a aby bylo minimalizováno riziko zranitelností, neoprávněného přístupu k datům nebo provozních narušení.

1.2 Stanovuje závazná pravidla bezpečného vývoje a postupy bezpečného kódování, které musí dodržovat všichni interní vývojáři, smluvní pracovníci a dodavatelé bez ohledu na velikost nebo složitost projektu.

1.3 Tato politika je navržena tak, aby chránila zákaznická data, předcházela narušení bezpečnosti dat a zajistila, že software vytvořený nebo upravený organizací nebo pro ni bude schopen úspěšně projít bezpečnostními audity, splnit právní požadavky (např. GDPR, směrnice NIS2, nařízení DORA) a podpořit certifikaci podle ISO/IEC 27001.

2. Rozsah

2.1 Tato politika se vztahuje na všechny osoby a subjekty zapojené do vývoje, úprav, nasazení nebo správy následujících položek jménem organizace:

2.1.1 webových stránek, aplikací nebo automatizačních nástrojů,

2.1.2 interně vyvinutých skriptů nebo softwaru,

2.1.3 kódu vytvořeného externími vývojáři nebo freelancery,

2.1.4 pluginů, knihoven a softwarových komponent integrovaných do produkčních systémů.

2.2 Pokrývá všechna prostředí používaná při vývojových činnostech, včetně:

2.2.1 vývojových a testovacích prostředí,

2.2.2 staging a předprodukčních prostředí,

2.2.3 produkčních systémů používaných ke spouštění vlastního vyvinutého kódu.

2.3 Tato politika dále upravuje nakládání s daty během vývoje a nasazení, zejména jakékoli použití produkčních dat v neprodukčních prostředích.

3. Cíle

3.1 Předcházet zavádění bezpečnostních chyb nebo zranitelností do vlastního softwaru nebo softwaru vyvinutého třetí stranou.

3.2 Zajistit, aby postupy bezpečného kódování a prevence zranitelností byly začleněny do každé fáze životního cyklu vývoje systémů.

3.3 Snižovat rizika spojená s využíváním open-source nebo komponent třetích stran prostřednictvím povinného řádného posouzení a průběžného sledování.

3.4 Vyžadovat formální přezkum kódu a bezpečnostní testování aplikací před vydáním.

3.5 Řídit přístup k vývojovým prostředím a zajistit jejich oddělení od produkčních systémů.

3.6 Splnit závazné požadavky vyplývající z mezinárodních norem a právních předpisů (např. ISO/IEC 27001, GDPR, nařízení DORA, směrnice NIS2).

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Schvaluje tuto politiku a odpovídá za její prosazování.

4.1.2 Zajišťuje, aby veškerý vývoj softwaru, interní i outsourcovaný, byl v souladu s touto politikou.

4.1.3 Přezkoumává a podepisuje smlouvy o vývoji nebo poskytování služeb obsahující ustanovení o bezpečném vývoji.

4.1.4 Ověřuje soulad dodavatelů prostřednictvím pravidelných kontrol nebo vyžádáním bezpečnostních důkazů.

4.2 interní vývojář nebo vlastník aplikace

4.2.1 Dodržuje postupy bezpečného kódování a bezpečného nasazení.

4.2.2 Používá kontrolní seznam bezpečného vývoje pro každý projekt.

4.2.3 Ověřuje bezpečnost všech použitých open-source komponent a komponent třetích stran.

4.2.4 Bezodkladně oznamuje generálnímu řediteli veškeré zjištěné zranitelnosti.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být generálním ředitelem přezkoumána nejméně jednou ročně za účelem:

9.1.1 ověření trvajícího souladu s ISO/IEC 27001, GDPR, směrnicí NIS2 a nařízením DORA,

9.1.2 zohlednění aktualizovaných hrozeb nebo změn v osvědčených postupech v odvětví pro bezpečný vývoj,

9.1.3 zajištění kompatibility s novými nástroji, platformami nebo vztahy s dodavateli.

9.2 Mimořádný přezkum musí být zahájen v případě:

9.2.1 jakéhokoli nahlášeného bezpečnostního incidentu souvisejícího se softwarem,

9.2.2 zavedení nového vývojového frameworku nebo hostingové platformy,

9.2.3 změny partnerů pro externí vývoj,

9.2.4 regulatorních změn ovlivňujících softwarové nebo bezpečnostní povinnosti.

9.3 Veškeré změny této politiky musí být:

9.3.1 zdokumentovány včetně data, shrnutí změny a schválení GM,

9.3.2 jednoznačně sděleny všem interním i externím pracovníkům zapojeným do vývoje,

9.3.3 uchovávány jako součást správy verzí politiky a historie změn organizace.

9.4 Aktualizované verze musí být snadno dostupné, a to buď prostřednictvím interních platforem, tištěné dokumentace nebo cloudových služeb přístupných dodavatelům.

10. Související politiky a vazby

10.1 Tato politika podporuje a je závislá na úspěšné implementaci několika dalších politik SME:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: stanoví odpovědnost za přiřazení a ověřování opatření bezpečného vývoje napříč projekty a dodavateli.

10.1.2 P4S – Politika řízení přístupu: poskytuje základní pravidla pro omezení přístupu do vývojových prostředí a repozitářů zdrojového kódu, včetně oddělení povinností.

10.1.3 P8S – Politika povědomí o bezpečnosti informací a školení: zajišťuje, aby interní vývojáři a smluvní pracovníci rozuměli postupům bezpečného kódování a souvisejícím bezpečnostním odpovědnostem.

10.1.4 P17S – Politika ochrany dat a soukromí: upřesňuje, jak musí být s osobními údaji nakládáno během vývoje, testování a protokolování, aby byl zajištěn soulad s GDPR.

10.1.5 P30S – Politika reakce na incidenty: definuje, jak musí být bezpečnostní incidenty související s vývojem hlášeny, posuzovány a řešeny, včetně expozice související s kódem.

10.2 Tyto politiky společně zajišťují, že bezpečný vývoj je dosažitelný a ověřitelný i v malé nebo technicky méně vyspělé organizaci.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Článek 8.1 – Vyžaduje zavedení provozních opatření, včetně bezpečného vývoje, která jsou v souladu s obchodními cíli a postojem k riziku.

11.2 ISO/IEC 27002

11.2.1 Opatření 8.25 – Doporučuje začlenit bezpečnost do celého životního cyklu softwaru, včetně správy zdrojového kódu, verzování a přístupu vývojářů.

11.2.2 Opatření 8.26 – Stanoví metody testování aplikací a ověřování bezpečnostních funkcí před uvedením do produkce.

11.2.3 Opatření 8.27 – Vyžaduje, aby externí vývojáři dodržovali stejné standardy vývoje a aby jejich bezpečnostní odpovědnosti byly jasně vymezeny.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 až SA-15 – Definují procesy bezpečného vývoje, včetně řízení přístupu vývojářů, testování, modelování hrozeb a dokumentace.

11.3.2 SI-10 – Vyžaduje, aby vývojáři identifikovali a zmírňovali běžné slabiny softwaru a tam, kde je to relevantní, používali automatizované nástroje.

11.4 GDPR (2016/679)

11.4.1 Článek 25 – „Ochrana osobních údajů již od návrhu a ve výchozím nastavení“ ukládá začlenit ochranu bezpečnosti a soukromí při návrhu a vývoji softwaru, zejména pokud jsou zpracovávány osobní údaje.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21 odst. 2 písm. a), e) a h) – Vyžaduje politiky bezpečného vývoje, dohled nad využíváním open-source a dokumentované zmírňování rizik souvisejících s aplikacemi u základních a významných subjektů.

11.6 nařízení DORA (2022/2554)

11.6.1 Články 6 odst. 7, 9 odst. 1 písm. c) a 10 odst. 2 písm. c) – Ukládají povinnosti týkající se bezpečnosti životního cyklu vývoje subjektům finančního sektoru, včetně SME, zejména u kritických ICT systémů.

11.7 COBIT 2019

11.7.1 BAI03 – „Řízení identifikace a tvorby řešení“ podporuje zavedení strukturovaných vývojových opatření zdůrazňujících bezpečnost, dohledatelnost a odolnost s ohledem na omezení SME.