					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P24					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**

1. Účel

1.1 Tato politika stanoví závazné bezpečnostní požadavky pro činnosti související s vývojem softwaru a systémů v rámci organizace, včetně interních projektů, outsourcovaného vývoje a integrace kódu třetích stran.

1.2 Cílem je zajistit, aby bezpečnost byla začleněna do celého životního cyklu vývoje softwaru (SDLC) a aby byly zranitelnosti před nasazením do produkčního prostředí identifikovány, zmírňovány a aby se jejich vzniku předcházelo.

1.3 Tato politika podporuje uplatňování kapitoly 8.1 normy ISO/IEC 27001:2022 a opatření 8.25–8.28 přílohy A tím, že standardizuje řízení bezpečného vývoje, postupy ověřování kódu a dohled nad vývojem třetích stran.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 software, aplikace, skripty, integrace a automatizační nástroje vyvíjené interně nebo externě

2.1.2 vývojové týmy, vlastníky produktů, týmy DevOps, QA, architekty, projektové manažery a externí pracovníky

2.1.3 prostředí SDLC včetně vývojových, testovacích, staging a předprodukčních systémů

2.1.4 open-source komponenty a komponenty třetích stran integrované do interních aplikací

2.1.5 software nasazený v on-premise infrastruktuře, privátním cloudu, hybridním prostředí nebo veřejném cloudu

2.2 Této politice podléhají všichni uživatelé a subjekty zapojení do vývoje, testování nebo nasazování systémů v rámci organizačního kontextu, včetně poskytovatelů řízených služeb (MSP) a dodavatelů platforem.

3. Cíle

3.1 Začlenit bezpečnostní opatření do všech fází vývoje softwaru, od návrhu po nasazení, tak, aby snižování rizik bylo proaktivní a průběžné.

3.2 Zabránit zavádění zneužitelných zranitelností, jako jsou chyby typu injection, nezabezpečená autentizace a expozice známým slabinám třetích stran.

3.3 Stanovit a uplatňovat postupy bezpečného kódování v souladu s OWASP, SANS CWE a doporučeními specifickými pro používané frameworky.

3.4 Zajistit, aby veškerý kód před nasazením prošel kolegiálním přezkumem, automatizovanou analýzou a bezpečnostním ověřením.

3.5 Řídit rizika vývoje vyplývající z outsourcovaných činností, začlenění kódu třetích stran a opětovného využití open-source softwaru.

3.6 Chránit vývojová, testovací a staging prostředí před neoprávněným přístupem a zabránit použití produkčních dat bez schváleného maskování dat nebo anonymizace.

3.7 Podporovat bezpečnostní povědomí u vývojářů, produktových manažerů a pracovníků QA prostřednictvím školení podle rolí a průběžných aktualizací o nově vznikajících hrozbách.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za tuto politiku a zajišťuje uplatňování požadavků bezpečného vývoje v celé organizaci.

4.1.2 Schvaluje standardy bezpečného kódování a smluvní ujednání pro vývoj třetích stran.

4.1.3 Schvaluje rozhodnutí o ošetření rizik pro nevyřešené nebo odložené zranitelnosti.

4.2 vedoucí bezpečnosti aplikací / manažer DevSecOps

4.2.1 Vytváří, udržuje a prosazuje směrnice pro bezpečné kódování.

4.2.2 Integruje statické a dynamické bezpečnostní testování do CI/CD pipeline.

4.2.3 Provádí bezpečnostní přezkumy kódu a stanovuje závazná nápravná opatření.

[... 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 přezkoumávána každoročně nebo častěji v reakci na:

9.1.1 významné změny metodik vývoje nebo nástrojů DevOps

9.1.2 závažné bezpečnostní incidenty vyplývající ze zranitelností aplikací

9.1.3 změny regulatorních požadavků souvisejících s bezpečným softwarem (např. GDPR, nařízení DORA)

9.1.4 nové oborové standardy nebo informace o hrozbách (např. OWASP Top 10, SLSA, MITRE CWE)

9.2 Přezkum politiky vede vedoucí bezpečnosti aplikací v koordinaci s CISO, softwarovými architekty, vedením QA a právním poradcem (pro dopady související s kódem třetích stran).

9.3 Veškeré změny musí být zaznamenány v registru řízení dokumentace ISMS, vedeny ve správě verzí a oznámeny dotčeným týmům prostřednictvím poznámek k vydání nebo povinného školení.

9.4 Předchozí verze musí být uchovávány v archivním repozitáři z důvodu právní obhajitelnosti a auditní dohledatelnosti.

10. Související politiky a vazby

10.1 P1 – Politika informační bezpečnosti. Stanoví strategický mandát pro začlenění bezpečnosti do všech informačních systémů, přičemž bezpečný vývoj představuje jedno ze základních provozních opatření.

10.2 P4 – Politika řízení přístupu. Definuje kontrolní opatření pro omezení přístupu do vývojových prostředí, repozitářů, build nástrojů a CI/CD pipeline.

10.3 P5 – Politika řízení změn. Zajišťuje, aby změny kódu, release a nasazení podléhaly řádnému schválení, plánování vrácení změn a ověření po nasazení.

10.4 P12 – Politika správy aktiv. Podporuje evidenci vývojových prostředí, zdrojových repozitářů a build systémů jako řízených aktiv podléhajících klasifikaci a ochraně.

10.5 P22 – Politika protokolování a monitorování. Vztahuje se na vývojové pipeline a zajišťuje, aby build procesy, povyšování kódu a události nasazení byly logovány, monitorovány a analyzovány z hlediska bezpečnostních anomálií.

10.6 P30 – Politika reakce na incidenty. Poskytuje rámec pro analýzu a reakci na bezpečnostní nedostatky zjištěné po nasazení nebo během bezpečnostního testování aplikací.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – provozní plánování a řízení: Vyžaduje začlenění procesů a opatření bezpečného vývoje do provozu.

11.2 ISO/IEC 27002:2022 – Opatření 8.25–8.28

11.2.1 Opatření 8.25 přílohy A – životní cyklus bezpečného vývoje: Vyžaduje formální začlenění bezpečnosti do návrhu a vývoje softwaru.

11.2.2 Opatření 8.26 přílohy A – požadavky na bezpečnost aplikací: Vyžaduje definování bezpečného kódování a bezpečnostních akceptačních kritérií.

11.2.3 Opatření 8.27 přílohy A – principy bezpečné architektury a návrhu systémů: Vyžaduje uplatnění principů bezpečnostního návrhu a zmírnění známých slabin.

11.2.4 Opatření 8.28 přílohy A – bezpečné kódování: Vyžaduje uplatňování zásad bezpečného kódování při vývoji softwaru.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 až SA-15: Zavádí strukturované postupy vývoje bezpečnosti aplikací, včetně požadavků na návrh, integritu kódu a testování.

11.3.2 SI-10 – validace vstupních dat: Zaměřuje se na obranné mechanismy bezpečného kódování.

11.3.3 SR-3 – ochrana dodavatelského řetězce: Vyžaduje prověrku softwaru třetích stran, komponent a poskytovatelů vývoje.

11.4 GDPR EU (2016/679)

11.4.1 Článek 25 – ochrana osobních údajů již od návrhu a ve výchozím nastavení: Ukládá začlenění bezpečnosti a ochrany soukromí do vývoje systémů.

11.4.2 Článek 32 – zabezpečení zpracování: Podporuje technická opatření, jako je validace vstupů, řízení přístupu a bezpečné nasazení.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21(2)(e–f): Vyžaduje postupy vývoje softwaru, které zahrnují řízení zranitelností, bezpečnost kódu a hlášení incidentů.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 9 – řízení rizik v oblasti ICT: Vyžaduje postupy bezpečného vývoje pro finanční subjekty, včetně opatření kvality softwaru a nápravy vad.

11.6.2 Článek 10 – kontinuita činností a testování: Podporuje důsledné testování a ověřování systémů ICT, včetně aplikací.

11.7 COBIT 2019

11.7.1 BAI03 – řídit identifikaci a tvorbu řešení: Upravuje návrh, vývoj a začlenění bezpečnosti do nových řešení.

11.7.2 BAI07 – řídit akceptaci změn a přechod do provozu: Zajišťuje bezpečné nasazení a vyhodnocení po nasazení.

11.7.3 DSS05 – řídit bezpečnostní služby: Uplatňuje bezpečnostní ověření na software a poskytování služeb.