					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P24					Názov dokumentu: **Politika bezpečného vývoja**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

1. Účel

1.1 Táto politika stanovuje záväzné bezpečnostné požiadavky na činnosti súvisiace s vývojom softvéru a systémov v rámci organizácie vrátane interných projektov, outsourcovaného vývoja a integrácie kódu tretích strán.

1.2 Cieľom je zabezpečiť, aby bezpečnosť bola začlenená do celého životného cyklu vývoja softvéru (SDLC) a aby zraniteľnosti boli identifikované, zmiernené a odstránené pred nasadením do produkčného prostredia.

1.3 Táto politika podporuje uplatňovanie požiadaviek ISO/IEC 27001:2022, kapitoly 8.1, a kontrol prílohy A 8.25–8.27 prostredníctvom štandardizácie správy a riadenia bezpečného vývoja, postupov validácie kódu a dohľadu nad vývojom realizovaným tretími stranami.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky:

2.1.1 interne alebo externe vyvíjané softvérové riešenia, aplikácie, skripty, integrácie a automatizačné nástroje

2.1.2 vývojové tímy, vlastníkov produktov, tímy DevOps, tímy QA, architektov, projektových manažérov a zmluvných pracovníkov

2.1.3 prostredia SDLC vrátane vývojových, testovacích, staging a predprodukčných systémov

2.1.4 open-source komponenty a komponenty tretích strán integrované do interných aplikácií

2.1.5 softvér nasadený on-premise, v súkromnom cloude, v hybridnom režime alebo vo verejnom cloudovom prostredí

2.2 Tejto politike podliehajú všetci používatelia a subjekty zapojení do vývoja, testovania alebo nasadzovania systémov v kontexte organizácie vrátane poskytovateľov spravovaných služieb a dodávateľov platforiem.

3. Ciele

3.1 Začleniť bezpečnostné kontrolné opatrenia do všetkých fáz vývoja softvéru od návrhu po nasadenie tak, aby znižovanie rizika bolo proaktívne a nepretržité.

3.2 Predchádzať zavedeniu zneužiteľných zraniteľností, ako sú chyby typu injection, nezabezpečená autentifikácia a vystavenie známym slabinám tretích strán.

3.3 Zaviesť a uplatňovať postupy bezpečného kódovania v súlade s OWASP, SANS CWE a usmerneniami špecifickými pre príslušné frameworky.

3.4 Zabezpečiť, aby každý kód pred nasadením prešiel vzájomným hodnotením, automatizovanou analýzou a bezpečnostnou validáciou.

3.5 Riadiť riziká vývoja vyplývajúce z outsourcovaných činností, začlenenia kódu tretích strán a opätovného použitia open-source softvéru.

3.6 Chrániť vývojové, testovacie a staging prostredia pred neoprávneným prístupom a zabrániť použitiu produkčných údajov bez schváleného maskovania údajov alebo anonymizácie.

3.7 Podporovať bezpečnostné povedomie medzi vývojármi, produktovými manažérmi a odborníkmi na zabezpečenie kvality prostredníctvom školení podľa rolí a priebežných aktualizácií o nových hrozbách.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje uplatňovanie požiadaviek bezpečného vývoja v celej organizácii.

4.1.2 Schvaľuje štandardy bezpečného kódovania a dohody o vývoji s tretími stranami.

4.1.3 Validuje rozhodnutia o ošetrení rizík pri neodstránených alebo odložených zraniteľnostiach.

4.2 vedúci aplikačnej bezpečnosti / manažér DevSecOps

4.2.1 Vypracúva, udržiava a presadzuje usmernenia pre bezpečné kódovanie.

4.2.2 Integruje statické a dynamické bezpečnostné testovanie do CI/CD pipeline.

4.2.3 Vykonáva bezpečnostné preskúmania kódu a určuje povinné nápravné opatrenia.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Táto politika musí byť preskúmaná najmenej raz ročne alebo častejšie v reakcii na:

9.1.1 významné zmeny metodík vývoja alebo nástrojov DevOps

9.1.2 významné bezpečnostné incidenty vyplývajúce zo zraniteľností aplikácií

9.1.3 zmeny regulačných požiadaviek týkajúcich sa bezpečného softvéru (napr. GDPR, DORA)

9.1.4 nové odvetvové normy alebo spravodajstvo o hrozbách (napr. OWASP Top 10, SLSA, MITRE CWE)

9.2 Preskúmanie politiky vedie vedúci aplikačnej bezpečnosti v koordinácii s CISO, softvérovými architektmi, vedením QA a právnym poradcom (v prípade dôsledkov súvisiacich s kódom tretích strán).

9.3 Všetky revízie musia byť zaznamenané v registri riadenia dokumentácie ISMS, musia podliehať riadeniu verzií a musia byť oznámené dotknutým tímom prostredníctvom poznámok k vydaniu alebo povinného školenia.

9.4 Staršie verzie musia byť uchovávané v archívnom repozitári na účely právnej obhájiteľnosti a auditnej sledovateľnosti.

10. Súvisiace politiky a väzby

10.1 P1 – Politika informačnej bezpečnosti. Stanovuje strategický mandát na začlenenie bezpečnosti do všetkých informačných systémov, pričom bezpečný vývoj predstavuje základné prevádzkové kontrolné opatrenie.

10.2 P4 – Politika riadenia prístupu. Definuje kontrolné opatrenia na obmedzenie prístupu do vývojových prostredí, repozitárov, build nástrojov a CI/CD pipeline.

10.3 P5 – Politika riadenia zmien. Zabezpečuje, aby zmeny kódu, vydania a nasadenia podliehali riadnemu schvaľovaniu, plánovaniu vrátenia zmien a overeniu po nasadení.

10.4 P12 – Politika správy aktív. Podporuje inventarizáciu aktív vývojových prostredí, zdrojových repozitárov a build systémov ako spravovaných aktív podliehajúcich klasifikácii a ochrane.

10.5 P22 – Politika logovania a monitorovania. Vzťahuje sa na vývojové pipeline a zabezpečuje, aby build procesy, presuny kódu a udalosti nasadenia boli logované, monitorované a analyzované z hľadiska bezpečnostných anomálií.

10.6 P30 – Politika reakcie na incidenty. Poskytuje rámec na analýzu a riešenie bezpečnostných nedostatkov zistených po nasadení alebo počas bezpečnostného testovania aplikácií.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: Vyžaduje integráciu procesov a kontrol bezpečného vývoja do prevádzky.

11.2 ISO/IEC 27002:2022 – Kontroly 8.25–8.27

11.2.1 Kontrola prílohy A 8.25 – Životný cyklus bezpečného vývoja: Vyžaduje formálne začlenenie bezpečnosti do návrhu a vývoja softvéru.

11.2.2 Kontrola prílohy A 8.26 – Bezpečnostné požiadavky na aplikácie: Vyžaduje definovanie požiadaviek na bezpečné kódovanie a bezpečnostných akceptačných kritérií.

11.2.3 Kontrola prílohy A 8.27 – Zásady bezpečnej architektúry a systémového inžinierstva: Vyžaduje uplatnenie princípov bezpečného návrhu a zmierňovanie známych slabín.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 až SA-15: Zavádza štruktúrované postupy bezpečného vývoja aplikácií vrátane požiadaviek na návrh, integritu kódu a testovanie.

11.3.2 SI-10 – Validácia vstupných údajov: Rieši opatrenia bezpečného kódovania.

11.3.3 SR-3 – Ochrana dodávateľského reťazca: Vyžaduje preverenie softvéru tretích strán, komponentov a poskytovateľov vývoja.

11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 25 – Ochrana údajov už pri návrhu a štandardne: Vyžaduje začlenenie bezpečnosti a ochrany súkromia do vývoja systémov.

11.4.2 Článok 32 – Bezpečnosť spracúvania: Podporuje technické opatrenia, ako sú validácia vstupov, riadenie prístupu a bezpečné nasadenie.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(e–f): Vyžaduje postupy vývoja softvéru, ktoré zahŕňajú riadenie zraniteľností, bezpečnosť kódu a nahlasovanie incidentov.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 9 – Riadenie rizík IKT: Vyžaduje postupy bezpečného vývoja pre finančné subjekty vrátane kontrol kvality softvéru a odstraňovania nedostatkov.

11.6.2 Článok 10 – Kontinuita činností a testovanie: Podporuje dôsledné testovanie a validáciu systémov IKT vrátane aplikácií.

11.7 COBIT 2019

11.7.1 BAI03 – Riadenie identifikácie riešení a ich tvorby: Upravuje návrh, vývoj a integráciu bezpečnosti do nových riešení.

11.7.2 BAI07 – Riadenie akceptácie zmien a prechodu: Zabezpečuje bezpečné nasadenie a hodnotenie po nasadení.

11.7.3 DSS05 – Riadenie bezpečnostných služieb: Uplatňuje bezpečnostnú validáciu na softvér a poskytovanie služieb.