					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P24S					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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Relevantné bezpečnostné kontroly pre prevádzkové postupy vrátane bezpečného vývoja
ISO/IEC 27002:2022	Kontroly 8.25–8.27	Zahŕňa životný cyklus bezpečného vývoja, testovanie a bezpečnostné zodpovednosti externých vývojárov
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Upravuje bezpečný životný cyklus vývoja softvéru, riadenie prístupu a odstraňovanie zraniteľností vo vývoji
GDPR EÚ	Článok 25	Vyžaduje ochranu súkromia už pri návrhu a štandardne pri vývoji softvéru
Smernica EÚ NIS2	Článok 21(2)(a), (e), (h)	Ukladá povinnosť mať politiky bezpečného vývoja, dohľad nad používaním open-source komponentov a zdokumentované zmierňujúce opatrenia
Nariadenie EÚ DORA	Články 6(7), 9(1)(c), 10(2)(c)	Bezpečnosť životného cyklu pre kritické IKT systémy vo finančnom sektore
COBIT 2019	BAI	Rámec pre štruktúrované, sledovateľné a odolné riadenie bezpečného vývoja

1. Účel

1.1 Táto politika zabezpečuje, aby bol všetok softvér, skripty a webové nástroje vytvorené alebo upravené organizáciou alebo jej externými partnermi vyvíjané bezpečným spôsobom, čím sa minimalizuje riziko zraniteľností, neoprávneného prístupu k údajom alebo narušenia prevádzky.

1.2 Stanovuje záväzné pravidlá bezpečného vývoja a bezpečného kódovania, ktoré musia dodržiavať všetci interní vývojári, zmluvní pracovníci a dodávatelia bez ohľadu na veľkosť alebo zložitosť projektu.

1.3 Táto politika je určená na ochranu údajov zákazníkov, predchádzanie porušeniam ochrany údajov a zabezpečenie toho, aby softvér vytvorený alebo prispôsobený organizáciou alebo pre organizáciu spĺňal požiadavky bezpečnostných auditov, právne požiadavky (napr. GDPR, NIS2, DORA) a podporoval certifikáciu podľa ISO/IEC 27001.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky osoby a subjekty, ktoré v mene organizácie vyvíjajú, prispôsobujú, nasadzujú alebo spravujú:

2.1.1 webové sídla, aplikácie alebo automatizačné nástroje,

2.1.2 interne vyvinuté skripty alebo softvér,

2.1.3 kód vytvorený externými vývojármi alebo osobami pracujúcimi na voľnej nohe,

2.1.4 pluginy, knižnice a softvérové komponenty integrované do produkčných systémov.

2.2 Zahŕňa všetky prostredia používané pri vývojových činnostiach vrátane:

2.2.1 vývojových a testovacích prostredí,

2.2.2 stagingových a predprodukčných prostredí,

2.2.3 produkčných systémov používaných na prevádzku vlastného vyvinutého kódu.

2.3 Politika upravuje aj nakladanie s údajmi počas vývoja a nasadenia, najmä akékoľvek použitie produkčných údajov v neprodukčných systémoch.

3. Ciele

3.1 Predchádzať zavedeniu bezpečnostných nedostatkov alebo zraniteľností do vlastného softvéru alebo softvéru vyvinutého tretími stranami.

3.2 Zabezpečiť, aby boli postupy bezpečného kódovania a prevencie zraniteľností integrované do každej fázy životného cyklu vývoja softvéru.

3.3 Znižovať riziká spojené s používaním open-source komponentov alebo komponentov tretích strán prostredníctvom povinného preverenia a priebežného sledovania.

3.4 Vyžadovať formálne preskúmanie kódu a bezpečnostné testovanie aplikácií pred vydaním.

3.5 Riadiť prístup k vývojovým prostrediam a zabezpečiť ich oddelenie od produkčných systémov.

3.6 Plniť záväzné požiadavky medzinárodných noriem a právnych predpisov (napr. ISO/IEC 27001, GDPR, DORA, NIS2).

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Schvaľuje túto politiku a je jej vlastníkom.

4.1.2 Zabezpečuje, aby bol všetok vývoj softvéru, interný aj outsourcovaný, v súlade s touto politikou.

4.1.3 Preskúmava a podpisuje zmluvy o vývoji alebo poskytovaní služieb, ktoré obsahujú ustanovenia o bezpečnom vývoji.

4.1.4 Overuje súlad dodávateľov prostredníctvom pravidelných kontrol alebo vyžiadaním bezpečnostných dôkazov.

4.2 Interný vývojár alebo vlastník aplikácie

4.2.1 Dodržiava postupy bezpečného kódovania a nasadzovania.

4.2.2 Pri každom projekte uplatňuje kontrolný zoznam bezpečného vývoja.

4.2.3 Overuje bezpečnosť všetkých použitých open-source komponentov alebo komponentov tretích strán.

4.2.4 Bezodkladne oznamuje GM všetky zistené zraniteľnosti.

[... 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 Túto politiku musí Generálny manažér preskúmať najmenej raz ročne s cieľom:

9.1.1 overiť trvalý súlad s ISO/IEC 27001, GDPR, NIS2 a DORA,

9.1.2 zohľadniť aktualizované hrozby alebo zmeny v osvedčených postupoch bezpečného vývoja,

9.1.3 zabezpečiť kompatibilitu s novými nástrojmi, platformami alebo vzťahmi s dodávateľmi.

9.2 Mimoriadne preskúmania sa musia vykonať pri:

9.2.1 akomkoľvek nahlásenom bezpečnostnom incidente súvisiacom so softvérom,

9.2.2 zavedení nového vývojového frameworku alebo hostingovej platformy,

9.2.3 zmene partnerov tretích strán pre vývoj,

9.2.4 regulačných zmenách, ktoré ovplyvňujú povinnosti týkajúce sa softvéru alebo bezpečnosti.

9.3 Všetky zmeny tejto politiky musia byť:

9.3.1 zdokumentované spolu s dátumom, súhrnom zmeny a schválením GM,

9.3.2 jasne komunikované všetkým interným a externým pracovníkom zapojeným do vývoja,

9.3.3 uchovávané ako súčasť riadenia verzií politiky a histórie zmien organizácie.

9.4 Aktualizované verzie musia byť ľahko dostupné prostredníctvom interných platforiem, tlačenej dokumentácie alebo cloudových služieb prístupných dodávateľom.

10. Súvisiace politiky a väzby

10.1 Táto politika podporuje a je závislá od úspešnej implementácie viacerých ďalších politík MSP:

10.1.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: stanovuje zodpovednosti za priradenie a overovanie kontrol bezpečnosti vývoja naprieč projektmi a dodávateľmi.

10.1.2 P4S – Politika riadenia prístupu: poskytuje základné pravidlá na obmedzenie prístupu k vývojovým prostrediam a repozitárom zdrojového kódu vrátane oddelenia povinností.

10.1.3 P8S – Politika zvyšovania povedomia a školení v oblasti informačnej bezpečnosti: zabezpečuje, aby interní vývojári a zmluvní pracovníci rozumeli postupom bezpečného kódovania a súvisiacim bezpečnostným zodpovednostiam.

10.1.4 P17S – Politika ochrany údajov a súkromia: objasňuje, ako sa musí nakladať s osobnými údajmi počas vývoja, testovania a procesov logovania, aby bol zabezpečený súlad s GDPR.

10.1.5 P30S – Politika reakcie na incidenty: definuje, ako sa musia nahlasovať, posudzovať a riešiť bezpečnostné incidenty súvisiace s vývojom vrátane vystavenia údajov súvisiaceho so zdrojovým kódom.

10.2 Každá z týchto politík spoločne prispieva k tomu, aby bol bezpečný vývoj dosiahnuteľný a overiteľný aj v malej alebo netechnickej organizácii.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje zavedenie prevádzkových kontrol vrátane bezpečného vývoja, ktoré sú v súlade s cieľmi organizácie a jej rizikovým profilom.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.25 – Odporúča integrovať bezpečnosť do celého životného cyklu softvéru vrátane správy zdrojového kódu, verziovania a prístupu vývojárov.

11.2.2 Kontrola 8.26 – Špecifikuje metódy testovania aplikácií a overovania bezpečnostných funkcií pred uvedením do produkčného prostredia.

11.2.3 Kontrola 8.27 – Vyžaduje, aby externí vývojári dodržiavali rovnaké štandardy vývoja a aby ich bezpečnostné zodpovednosti boli jasne definované.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 až SA-15 – Definujú procesy bezpečného vývoja vrátane riadenia prístupu vývojárov, testovania, modelovania hrozieb a dokumentácie.

11.3.2 SI-10 – Vyžaduje, aby vývojári identifikovali a zmierňovali bežné bezpečnostné slabiny softvéru a podľa potreby používali automatizované nástroje.

11.4 GDPR EÚ (2016/679)

11.4.1 Článok 25 – „Ochrana údajov už pri návrhu a štandardne“ vyžaduje integrovať bezpečnostné opatrenia a ochranu súkromia počas návrhu a vývoja softvéru, najmä ak sa spracúvajú osobné údaje.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(a), (e) a (h) – Vyžaduje politiky bezpečného vývoja, dohľad nad používaním open-source komponentov a zdokumentované zmierňovanie rizík súvisiacich s aplikáciami v základných a dôležitých subjektoch.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Články 6(7), 9(1)(c) a 10(2)(c) – Ukladajú povinnosti týkajúce sa bezpečnosti životného cyklu vývoja pre subjekty finančného sektora vrátane MSP, najmä pre kritické IKT systémy.

11.7 COBIT 2019

11.7.1 BAI03 – „Riadenie identifikácie a tvorby riešení“ podporuje implementáciu štruktúrovaných kontrol vývoja, ktoré zdôrazňujú bezpečnosť, sledovateľnosť a odolnosť, s prihliadnutím na obmedzenia MSP.