					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P28S					Názov dokumentu: **Politika outsourcovaného 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	Kapitoly 5.1, 6.1, 8	Uplatniteľné kontroly ISMS a kontroly súvisiace s dodávateľmi
ISO/IEC 27002:2022	Kontroly 5.19, 5.20, 8.25–8.27	Kontroly dodávateľov a bezpečného životného cyklu vývoja
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Požiadavky na obstarávanie, dodávateľský reťazec, bezpečný vývoj a zmluvy s dodávateľmi
GDPR EÚ	Článok 28	Zmluvné požiadavky a požiadavky na ochranu údajov pri spracúvaní treťou stranou
NIS2 EÚ	Článok 21(2)(a), (h)	Kontroly bezpečnosti dodávateľského reťazca a bezpečného vývoja aplikácií
DORA EÚ	Článok 10	Riadenie rizík IKT tretích strán vrátane outsourcovaného vývoja
COBIT 2019	BAI03, DSS05	Požiadavky na externý vývoj a externých poskytovateľov IT služieb

1. Účel

1.1 Táto politika zabezpečuje, aby sa všetok outsourcovaný vývoj softvéru bez ohľadu na to, či ho vykonávajú freelanceri, agentúry alebo poskytovatelia tretích strán, realizoval bezpečne, na základe zmluvného riadenia a v súlade s príslušnými právnymi, regulačnými a audítorskými požiadavkami.

1.2 Chráni organizáciu pred rizikami súvisiacimi s nezabezpečeným kódom, nejasným vlastníctvom, vystavením údajov a nedostatočným riadením dodávateľov tým, že zavádza záväzné štandardy vývoja a dohľad nad dodávateľmi aj v prípade, keď organizácia nemá vyhradené IT oddelenie.

1.3 Táto politika podporuje certifikáciu podľa ISO/IEC 27001:2022 tým, že stanovuje jasne definované očakávania pre vývoj, priradenie zodpovednosti a zdokumentované opatrenia pre vývojové činnosti tretích strán.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých externých vývojárov vrátane freelancerov a vývojových agentúr,

2.1.2 akékoľvek vývojové práce zahŕňajúce interné nástroje, verejne prístupné systémy, softvérové aplikácie alebo automatizáciu podnikových procesov,

2.1.3 zamestnancov zodpovedných za výber, riadenie alebo dohľad nad externými vývojármi,

2.1.4 akúkoľvek integráciu systémov tretích strán, skriptovanie alebo vývoj, ktoré interagujú s údajmi alebo systémami spoločnosti.

2.2 Zahŕňa aj akúkoľvek stranu alebo platformu s prístupom k prihlasovacím údajom spoločnosti, dátovým úložiskám, repozitárom zdrojového kódu, testovacím prostrediam alebo produkčným systémom.

3. Ciele

3.1 Zabezpečiť, aby všetok outsourcovaný vývoj dodržiaval princípy bezpečného programovania a aby vývojári boli zmluvne zaviazaní dodržiavať zdokumentované štandardy a ustanovenia o dôvernosti.

3.2 Zaviesť vlastníctvo všetkých výstupov — kódu, aktív, prihlasovacích údajov a dokumentácie — tak, aby bol zabezpečený úplný prevod práv na spoločnosť a sledovateľné odovzdanie pri ukončení projektu.

3.3 Predchádzať bežným vývojovým rizikám vrátane opätovného použitia proprietárneho kódu, útokov na dodávateľský reťazec prostredníctvom knižníc, používania nepodporovaných frameworkov a neprevereného administrátorského prístupu.

3.4 Vyžadovať pred začatím spolupráce dokumentáciu pre každý outsourcovaný projekt vrátane zmlúv, dohôd o mlčanlivosti a minimálnych bezpečnostných požiadaviek.

3.5 Chrániť údaje zákazníkov, systémy a interné procesy prostredníctvom dôsledného dohľadu nad vývojom, testovania po dodaní a bezpečného riadenia systémového prístupu.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Schvaľuje všetky vzťahy s dodávateľmi a podpisuje zmluvy o vývoji.

4.1.2 Zabezpečuje, aby sa všetok outsourcovaný vývoj riadil touto politikou.

4.1.3 Po ukončení projektu odoberá prístupy do systémov spoločnosti.

4.1.4 Preskúmava dokumentáciu a výsledky po dodaní.

4.2 Vlastník projektu (spravidla interný zamestnanec alebo určený koordinátor)

4.2.1 Riadi každodennú koordináciu s externým vývojárom.

4.2.2 Overuje, že sú splnené funkčné požiadavky a že výstupy boli otestované.

4.2.3 Zabezpečuje bezpečné odovzdanie kódu a prihlasovacích údajov.

4.2.4 Oznamuje GM akékoľvek problémy alebo incidenty súvisiace s vývojom.

[... 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 Ročné preskúmanie

9.1.1 Túto politiku musí Generálny manažér (GM) preskúmať najmenej raz ročne. Preskúmanie zabezpečuje, že politika naďalej spĺňa:

9.1.1.1 požiadavky certifikácie ISO/IEC 27001,

9.1.1.2 zmeny zákonných povinností (napr. článok 28 GDPR, článok 10 DORA),

9.1.1.3 aktuálne postupy vývoja na úrovni MSP a riziká tretích strán.

9.2 Priebežné preskúmania

9.2.1 Preskúmania politiky sa musia vykonať aj vtedy, keď:

9.2.1.1 je zavedený nový dodávateľ alebo platforma pre outsourcovaný vývoj,

9.2.1.2 dôjde k významnému incidentu súvisiacemu s outsourcovaným vývojom,

9.2.1.3 dôjde k podstatným zmenám v používaných nástrojoch, platformách alebo prostrediach.

9.3 Proces preskúmania

9.3.1 GM je zodpovedný za:

9.3.1.1 overenie, že zmluvy, NDA a procesy riadenia prístupu zostávajú účinné,

9.3.1.2 potvrdenie, že aktuálni dodávatelia a freelanceri sú v súlade s politikou,

9.3.1.3 úpravu ustanovení na základe spätnej väzby z predchádzajúcich projektov alebo incidentov.

9.4 Riadenie verzií a komunikácia

9.4.1 Všetky zmeny musia byť:

9.4.1.1 zaznamenané s dátumom, dôvodom a opisom zmeny,

9.4.1.2 schválené GM a doplnené do histórie verzií,

9.4.1.3 oznámené všetkým zamestnancom alebo vlastníkom projektov spolupracujúcim s externými vývojármi,

9.4.1.4 podľa potreby opätovne distribuované všetkým dotknutým dodávateľom a tretím stranám.

10. Súvisiace politiky a väzby

10.1 Táto politika priamo podporuje implementáciu týchto politík zosúladených pre MSP a zároveň je od nich závislá:

10.1.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: Spresňuje, kto je zodpovedný za schválenie dodávateľov, riadenie prístupu a akceptáciu rizika pri využívaní externých vývojárov.

10.1.2 P4S – Politika riadenia prístupu: Definuje správne vytváranie, obmedzovanie a rušenie používateľských účtov a administrátorského prístupu používaných počas outsourcovaného vývoja.

10.1.3 P8S – Politika povedomia a školenia v oblasti informačnej bezpečnosti: Zabezpečuje, aby interní zamestnanci rozumeli tomu, ako bezpečne koordinovať prácu s externými vývojármi vrátane nakladania s prihlasovacími údajmi a projektovými súbormi.

10.1.4 P17S – Politika ochrany údajov a súkromia: Stanovuje bezpečnostné a právne požiadavky na nakladanie s osobnými údajmi, ktoré môžu externí vývojári spracúvať podľa GDPR.

10.1.5 P24S – Politika bezpečného vývoja: Určuje, ako musí interný aj externý vývoj dodržiavať postupy bezpečného programovania a preverovanie knižníc a frameworkov.

10.1.6 P30S – Politika reakcie na incidenty: Uplatňuje sa, ak outsourcovaný vývoj vedie k bezpečnostným incidentom alebo zraniteľnostiam, a usmerňuje koordinované vyšetrovanie a nápravné opatrenia.

10.2 Tieto politiky sa musia implementovať súbežne, aby outsourcovaný vývoj nevytváral neriadené riziko ani neporušoval povinnosti súladu MSP.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – Organizácie musia posúdiť a ošetriť riziká informačnej bezpečnosti súvisiace s dodávateľmi.

11.1.2 Kapitola 8.1 – Vyžaduje prevádzkové plánovanie a riadenie vrátane služieb tretích strán, ako je outsourcovaný vývoj.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.19 – Odporúča hodnotiť schopnosť dodávateľov plniť požiadavky informačnej bezpečnosti.

11.2.2 Kontrola 5.20 – Podporuje pravidelné monitorovanie a pravidelné preskúmanie služieb tretích strán.

11.2.3 Kontroly 8.25–8.27 – Stanovujú postupy bezpečného životného cyklu vývoja uplatniteľné na outsourcovaný vývoj.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Vyžaduje, aby stratégie obstarávania zahŕňali opatrenia informačnej bezpečnosti.

11.3.2 SA-9 – Rieši externý vývoj systémov a riziká dodávateľského reťazca.

11.3.3 SA-11 – Definuje postupy bezpečného vývoja vrátane preskúmania kódu a odstraňovania nedostatkov.

11.3.4 SA-15 – Podporuje používanie automatizovaných nástrojov na detekciu nedostatkov a zabezpečenie kvality softvéru.

11.3.5 SR-3 – Vyžaduje, aby zmluvy s dodávateľmi obsahovali požiadavky kybernetickej bezpečnosti.

11.4 Všeobecné nariadenie EÚ o ochrane údajov (GDPR)

11.4.1 Článok 28 – Vyžaduje, aby zmluvy so sprostredkovateľmi obsahovali primerané ochranné opatrenia na ochranu údajov; to sa priamo vzťahuje na vývojárov, ktorí spracúvajú osobné údaje alebo k nim pristupujú.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(a), (h) – Vyžaduje kontroly bezpečnosti dodávateľského reťazca a postupy bezpečného vývoja softvéru pre dotknutých poskytovateľov digitálnych služieb vrátane MSP, ak je to uplatniteľné.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 10 – Vyžaduje riadenie rizík IKT tretích strán vrátane zmlúv o vývoji, bezpečnostných povinností a kontrol rizík súvisiacich s poskytovateľmi tretích strán.

11.7 COBIT 2019

11.7.1 BAI03 – Riadenie identifikácie a tvorby riešení – zabezpečuje, aby externý vývoj spĺňal obchodné požiadavky a bezpečnostné očakávania.

11.7.2 DSS05 – Riadenie bezpečnostných služieb – vyžaduje, aby externé bezpečnostné služby a poskytovatelia vývoja fungovali podľa uplatňovaných bezpečnostných pravidiel a pod dohľadom.