					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P28S					Název dokumentu: **Politika outsourcovaného 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	Kapitola / článek	Komentář
ISO/IEC 27001:2022	Kapitoly 5.1, 6.1, 8	Relevantní opatření ISMS a opatření související s dodavateli
ISO/IEC 27002:2022	Opatření 5.19, 5.20, 8.25–8.27	Opatření pro dodavatele a bezpečný životní cyklus vývoje
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-11, SA-15, SR-3	Požadavky na pořizování, dodavatelský řetězec, bezpečný vývoj a smluvní ujednání s dodavateli
GDPR	Článek 28	Smluvní požadavky a požadavky na ochranu osobních údajů při zpracování třetí stranou
směrnice NIS2	Článek 21(2)(a), (h)	Opatření k zabezpečení dodavatelského řetězce a bezpečný vývoj aplikací
nařízení DORA	Článek 10	Řízení rizik třetích stran v oblasti ICT, včetně outsourcovaného vývoje
COBIT 2019	BAI03, DSS05	Požadavky na externí vývoj a externí poskytovatele IT služeb

1. Účel

1.1 Tato politika zajišťuje, aby veškerý outsourcovaný vývoj softwaru, ať už jej provádějí freelanceři, agentury nebo poskytovatelé služeb třetích stran, probíhal bezpečně, byl smluvně ošetřen a byl v souladu s příslušnými právními, regulatorními a auditními požadavky.

1.2 Tato politika chrání organizaci před riziky souvisejícími s nezabezpečeným kódem, nejasným vlastnictvím, expozicí dat a nedostatečným řízením dodavatelů tím, že stanoví vymahatelné standardy vývoje a dohled nad dodavateli, a to i v případě neexistence specializovaného IT oddělení.

1.3 Tato politika podporuje certifikaci podle ISO/IEC 27001:2022 tím, že stanoví jasně definovaná očekávání pro vývoj, odpovědnost a dokumentovaná opatření pro činnosti vývoje prováděné třetími stranami.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny externí vývojáře, včetně freelancerů a vývojových agentur,

2.1.2 veškeré vývojové činnosti zahrnující interní nástroje, webové stránky přístupné z veřejných sítí, softwarové aplikace nebo podnikovou automatizaci,

2.1.3 pracovníky odpovědné za výběr, řízení nebo dohled nad externími vývojáři,

2.1.4 jakoukoli integraci systémů třetích stran, skriptování nebo vývoj, které interagují s firemními daty nebo systémy.

2.2 Zahrnuje také jakoukoli stranu nebo platformu s přístupem k firemním přihlašovacím údajům, datovým repozitářům, repozitářům zdrojového kódu, testovacím prostředím nebo produkčním systémům.

3. Cíle

3.1 Zajistit, aby veškerý outsourcovaný vývoj dodržoval zásady bezpečného kódování a aby vývojáři byli smluvně zavázáni dodržovat dokumentované standardy a ustanovení o mlčenlivosti.

3.2 Stanovit vlastnictví všech výstupů — kódu, aktiv, přihlašovacích údajů a dokumentace — tak, aby byl zajištěn úplný převod práv na společnost a dohledatelné předání při ukončení projektu.

3.3 Předcházet běžným rizikům vývoje, včetně opětovného použití proprietárního kódu, útoků na dodavatelský řetězec prostřednictvím knihoven, použití nepodporovaných frameworků a neprověřeného administrátorského přístupu.

3.4 Vyžadovat před zahájením spolupráce dokumentaci ke každému outsourcovanému projektu, včetně smluv, dohod o mlčenlivosti a minimálních bezpečnostních očekávání.

3.5 Chránit zákaznická data, systémy a interní procesy prostřednictvím důsledného dohledu nad vývojem, testování po dodání a bezpečného řízení systémových přístupů.

4. Role a odpovědnosti

4.1 Generální ředitel (GM)

4.1.1 schvaluje všechny vztahy s dodavateli a podepisuje smlouvy o vývoji,

4.1.2 zajišťuje, aby veškerý outsourcovaný vývoj probíhal v souladu s touto politikou,

4.1.3 po dokončení projektu odebírá přístup do firemních systémů,

4.1.4 provádí přezkum dokumentace a výsledků po dodání.

4.2 Vlastník projektu (obvykle interní zaměstnanec nebo určený koordinátor)

4.2.1 zajišťuje každodenní koordinaci s externím vývojářem,

4.2.2 ověřuje splnění funkčních požadavků a otestování výstupů,

4.2.3 zajišťuje bezpečné předání kódu a přihlašovacích údajů,

4.2.4 oznamuje GM veškeré problémy nebo incidenty související s vývojem.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Každoroční přezkum

9.1.1 Tato politika musí být přezkoumána generálním ředitelem (GM) nejméně jednou ročně. Přezkum ověřuje, že politika nadále splňuje:

9.1.1.1 požadavky na certifikaci podle ISO/IEC 27001,

9.1.1.2 změny právních povinností (např. článek 28 GDPR, článek 10 nařízení DORA),

9.1.1.3 aktuální postupy vývoje na úrovni SME a rizika třetích stran.

9.2 Mimořádné přezkumy

9.2.1 Přezkum politiky musí proběhnout také tehdy, pokud:

9.2.1.1 je zařazen nový dodavatel nebo platforma pro outsourcovaný vývoj,

9.2.1.2 dojde k významnému incidentu souvisejícímu s outsourcovaným vývojem,

9.2.1.3 nastanou podstatné změny používaných nástrojů, platforem nebo prostředí.

9.3 Proces přezkumu

9.3.1 GM odpovídá za:

9.3.1.1 ověření, že smlouvy, dohody o mlčenlivosti a procesy řízení přístupu zůstávají účinné,

9.3.1.2 potvrzení, že stávající dodavatelé a freelanceři postupují v souladu s politikou,

9.3.1.3 úpravu podmínek na základě zpětné vazby z předchozích projektů nebo incidentů.

9.4 Řízení verzí a komunikace

9.4.1 Všechny změny musí být:

9.4.1.1 zaznamenány s datem, důvodem a popisem změny,

9.4.1.2 schváleny GM a doplněny do historie verzí,

9.4.1.3 oznámeny všem pracovníkům nebo vlastníkům projektů spolupracujícím s externími vývojáři,

9.4.1.4 v případě potřeby znovu distribuovány všem dotčeným dodavatelům a třetím stranám.

10. Související politiky a vazby

10.1 Tato politika přímo podporuje implementaci následujících politik uzpůsobených pro SME a je na jejich implementaci závislá:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: upřesňuje, kdo odpovídá za schvalování dodavatelů, řízení přístupu a akceptaci rizika při využívání externích vývojářů.

10.1.2 P4S – Politika řízení přístupu: stanoví správné zřizování, omezení a ukončení uživatelských účtů a administrátorského přístupu používaných v rámci outsourcovaného vývoje.

10.1.3 P8S – Politika povědomí o bezpečnosti informací a školení: zajišťuje, aby interní pracovníci rozuměli tomu, jak bezpečně koordinovat činnosti s externími vývojáři, včetně nakládání s přihlašovacími údaji a projektovými soubory.

10.1.4 P17S – Politika ochrany dat a soukromí: stanoví bezpečnostní a právní požadavky na nakládání s osobními údaji, které mohou být externími vývojáři zpracovávány podle GDPR.

10.1.5 P24S – Politika bezpečného vývoje: stanoví, jak musí interní i externí vývoj dodržovat postupy bezpečného kódování a prověřování knihoven a frameworků.

10.1.6 P30S – Politika reakce na incidenty: je vyžadována, pokud outsourcovaný vývoj vede k bezpečnostním incidentům nebo zranitelnostem, a poskytuje rámec pro koordinované vyšetřování a nápravu.

10.2 Tyto politiky musí být implementovány souběžně, aby outsourcovaný vývoj nevytvářel neřízené riziko ani nevedl k porušení povinností SME v oblasti souladu.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – Organizace musí vyhodnocovat a ošetřovat rizika bezpečnosti informací související s dodavateli.

11.1.2 Kapitola 8.1 – Vyžaduje provozní plánování a řízení, včetně služeb třetích stran, jako je outsourcovaný vývoj.

11.2 ISO/IEC 27002

11.2.1 Opatření 5.19 – Doporučuje hodnotit schopnost dodavatelů plnit požadavky bezpečnosti informací.

11.2.2 Opatření 5.20 – Podporuje pravidelné monitorování a pravidelný přezkum služeb třetích stran.

11.2.3 Opatření 8.25–8.27 – Vymezují postupy bezpečného životního cyklu vývoje použitelné pro outsourcovaný vývoj.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-4 – Vyžaduje, aby strategie pořizování zahrnovaly opatření informační bezpečnosti.

11.3.2 SA-9 – Řeší externí vývoj systémů a rizika dodavatelského řetězce.

11.3.3 SA-11 – Stanoví postupy bezpečného vývoje, včetně přezkumů kódu a nápravy vad.

11.3.4 SA-15 – Podporuje použití automatizovaných nástrojů pro detekci vad a zajištění kvality softwaru.

11.3.5 SR-3 – Vyžaduje, aby smluvní ujednání s dodavateli obsahovala požadavky na kybernetickou bezpečnost.

11.4 Obecné nařízení EU o ochraně osobních údajů (GDPR)

11.4.1 Článek 28 – Vyžaduje, aby smlouvy se zpracovateli z řad třetích stran zajišťovaly odpovídající opatření na ochranu osobních údajů; to se přímo vztahuje na vývojáře zpracovávající osobní údaje nebo k nim přistupující.

11.5 směrnice EU NIS2 (2022/2555)

11.5.1 Článek 21(2)(a), (h) – Vyžaduje opatření k zabezpečení dodavatelského řetězce a postupy bezpečného vývoje softwaru u poskytovatelů digitálních služeb spadajících do působnosti, včetně SME, pokud je to relevantní.

11.6 nařízení EU DORA

11.6.1 Článek 10 – Vyžaduje řízení rizik třetích stran v oblasti ICT, včetně smluv o vývoji, bezpečnostních povinností a kontrol rizik souvisejících s poskytovateli třetích stran.

11.7 COBIT 2019

11.7.1 BAI03 – Řízení identifikace a tvorby řešení – zajišťuje, aby externí vývoj splňoval obchodní požadavky a bezpečnostní očekávání.

11.7.2 DSS05 – Řízení bezpečnostních služeb – vyžaduje, aby externí bezpečnostní služby a poskytovatelé vývoje fungovali podle uplatňovaných bezpečnostních pravidel a pod dohledem.