					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P28					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	Kapitola 8.1	N/A
ISO/IEC 27002:2022	Opatření 5.19-5.22, 8	N/A
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	N/A
GDPR	Články 28, 32	N/A
směrnice NIS2	Články 21(2)(a), (h), 23	N/A
nařízení DORA	Články 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Účel

1.1 Tato politika stanoví závazná opatření pro outsourcování vývoje softwaru nebo systémů externím dodavatelům, smluvním pracovníkům nebo agenturám tak, aby byly bezpečnostní postupy začleněny do celého životního cyklu vývoje.

1.2 Jejím cílem je předcházet zranitelnostem, ztrátě dat, zpřístupnění duševního vlastnictví (IP) a porušení souladu vyplývajícím ze zapojení externích vývojových subjektů.

1.3 Tato politika stanoví požadavky na řízení dodavatelů, standardy bezpečného kódování, řízení přístupu, oznamovací povinnosti, monitorování a offboarding po ukončení smluvního vztahu s cílem zachovat důvěrnost, integritu a dostupnost vyvíjeného softwaru.

2. Rozsah

2.1 Tato politika se vztahuje na všechny organizační útvary, které zapojují externí subjekty do vývoje softwaru nebo systémů, včetně:

2.1.1 webových aplikací, mobilních aplikací, vestavěných systémů, API, skriptů, automatizačních workflow nebo modulů platforem,

2.1.2 zakázkového vývoje pro interní platformy, systémy určené zákazníkům nebo komerční produkty,

2.1.3 spolupráce s externími vývojáři, freelancery, agenturami nebo offshore týmy.

2.2 Tato politika se rovněž vztahuje na jakýkoli externí subjekt, který během vývoje přistupuje ke zdrojovému kódu, testovacím prostředím nebo CI/CD pipeline.

2.3 Tyto požadavky jsou závazné bez ohledu na typ smluvního vztahu, metodiku vývoje nebo geografické umístění outsourcovaného poskytovatele.

3. Cíle

3.1 Uplatňovat postupy bezpečného životního cyklu vývoje softwaru (SDLC) u všech outsourcovaných zakázek od plánování až po ověření po nasazení.

3.2 Zajistit, aby všechny smlouvy s externími vývojáři obsahovaly závazná ustanovení týkající se ochrany dat, bezpečného kódování a zachování práv k duševnímu vlastnictví.

3.3 Stanovit požadavky na řízení přístupu, monitorování a audit vývojářů třetích stran, kteří pracují s interními systémy.

3.4 Chránit organizaci před hrozbami v dodavatelském řetězci, porušením právních povinností a poškozením dobré pověsti souvisejícím se softwarem vyvinutým externě.

3.5 Udržovat trvalý soulad s bezpečnostními rámci, včetně ISO/IEC 27001, NIST, GDPR, NIS2, DORA a COBIT 2019.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje projekty outsourcovaného vývoje s vysokým rizikem a odůvodněné výjimky z této politiky.

4.1.2 Zajišťuje, aby rozhodnutí o outsourcingu byla v souladu se strategickými cíli a apetitem k riziku organizace.

4.2 Ředitel informační bezpečnosti (CISO)

4.2.1 Schvaluje zařazení dodavatelů z hlediska bezpečnosti.

4.2.2 Definuje požadavky na bezpečnostní opatření pro outsourcované zakázky a přezkoumává hlášení incidentů.

[... 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 přezkoumána nejméně jednou ročně nebo častěji za následujících okolností:

9.1.1 zavedení nových modelů outsourcingu vývoje, dodavatelů nebo jurisdikcí,

9.1.2 aktualizace regulatorních rámců, jako jsou GDPR, NIS2 nebo DORA,

9.1.3 po bezpečnostním incidentu zahrnujícím outsourcovaný kód, přístup nebo výstupy,

9.1.4 v návaznosti na zjištění interního auditu nebo zlepšování ISMS.

9.2 Ředitel informační bezpečnosti (CISO) odpovídá za zahájení a koordinaci přezkumu politiky po konzultaci s:

9.2.1.1 útvary právního a nákupu (z hlediska souladu a smluvního zajištění),

9.2.1.2 vlastníky projektů a produktů (z hlediska provozní proveditelnosti),

9.2.1.3 týmem informační bezpečnosti (z hlediska aktualizace hrozeb a opatření),

9.2.1.4 vrcholovým vedením (pro konečné schválení).

9.3 Všechny aktualizace politiky musí být:

9.3.1.1 vedeny v režimu správy verzí a uloženy v určeném repozitáři dokumentace,

9.3.1.2 oznámeny zainteresovaným stranám zapojeným do činností outsourcovaného vývoje,

9.3.1.3 provázány s aktualizacemi souvisejících politik nebo procesní dokumentace.

9.4 Každou verzi politiky musí doprovázet přehled změn, aby byla zajištěna dohledatelnost úprav a schválení.

10. Související politiky a vazby

10.1 Tato politika podporuje níže uvedené související dokumenty a současně je jimi podporována:

10.1.1 P1 - P01 Politika informační bezpečnosti: stanoví podnikové zásady bezpečnosti použitelné v interním vývoji i vývoji realizovaném třetími stranami.

10.1.2 P5 - Politika řízení změn: zajišťuje, aby všechny změny související s nasazením z outsourcovaných kódových základen byly před implementací přezkoumány a schváleny.

10.1.3 P13 - Politika klasifikace dat a označování: určuje, jak jsou citlivá data identifikována před jejich zpřístupněním vývojovým dodavatelům nebo repozitářům.

10.1.4 P18 - Politika kryptografických opatření: stanoví, jak musí být během vývoje a předávání nakládáno s klíči, tajnými údaji a citlivými přihlašovacími údaji.

10.1.5 P24 - Politika bezpečného vývoje: definuje základní požadavky pro interní i externí postupy vývoje softwaru.

10.1.6 P30 - Politika reakce na incidenty: upravuje, jak jsou porušení bezpečnosti nebo bezpečnostní problémy související s outsourcovaným vývojem eskalovány, vyšetřovány a řešeny.

10.1.7 P33 - Politika monitorování auditu a souladu: stanoví požadavky na přezkum outsourcovaných vývojových činností během auditů nebo přezkumů souladu.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s mezinárodně uznávanými bezpečnostními rámci a právními předpisy, aby bylo zajištěno bezpečné outsourcování vývoje softwaru a postupů řízení dodavatelů.

11.2 ISO/IEC 27001

11.2.1 Kapitola 8.1 - Operativní plánování a řízení: stanoví procesní opatření pro bezpečný vývoj a dodávky třetích stran.

11.3 ISO/IEC 27002:2022 - Opatření 5.19 až 5.21, 8

11.3.1 Příloha A, Opatření 5.19 - Řízení vztahů s dodavateli: vyžaduje formální dohody obsahující ustanovení o bezpečnosti a souladu.

11.3.2 Příloha A, Opatření 5.20 - Řešení bezpečnosti informací ve smlouvách s dodavateli: zajišťuje, aby byla do smluv zahrnuta opatření specifická pro vývoj.

11.3.3 Příloha A, Opatření 5.21 - Řízení poskytování služeb dodavatelů: zahrnuje monitorování výstupů a rizik vývoje realizovaného třetími stranami.

11.3.4 Příloha A, Opatření 8.27 - Outsourcovaný vývoj: vyžaduje definované bezpečnostní požadavky a řízení přístupu k externě vyvíjenému softwaru.

11.3.5 Tato opatření stanoví strukturované požadavky pro výběr, smluvní zajištění a dohled nad outsourcovanými vývojáři, včetně postupů bezpečného vývoje, nakládání s kódem a ověřování výkonnosti.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Proces pořizování: vyžaduje, aby byly požadavky na bezpečný vývoj definovány již v době pořizování.

11.4.2 SA-9 - Služby externích systémů: upravuje, jak mají vývojáři třetích stran bezpečně pracovat s interními službami.

11.4.3 SA-10 - Řízení konfigurace vývojáře: je v souladu s povinnostmi externích týmů v oblasti správy verzí, přístupu ke kódu a sledování změn.

11.5 GDPR (2016/679)

11.5.1 Článek 28 - Povinnosti zpracovatele: vyžaduje, aby smlouvy s vývojáři třetích stran stanovily bezpečnostní požadavky, opatření a požadavky na audit při nakládání s osobními údaji.

11.5.2 Článek 32 - Zabezpečení zpracování: vyžaduje přiměřená ochranná opatření (např. šifrování, řízení přístupu) při vývoji systémů, které zpracovávají osobní údaje.

11.6 směrnice NIS2 (2022/2555)

11.6.1 Články 21(2)(a), (h), 23: vyžadují, aby byly postupy bezpečného vývoje uplatňovány v rámci zapojení třetích stran a digitálních dodavatelských řetězců, včetně dohledu a technického ověření.

11.7 nařízení DORA (2022/2554)

11.7.1 Články 28(1), (2): vyžadují, aby finanční subjekty řídily ICT rizika třetích stran prostřednictvím smluvních opatření a dohledu nad bezpečným vývojem, zejména u kritického outsourcovaného vývoje.

11.8 COBIT 2019

11.8.1 APO10 - Řízení dodavatelů: stanoví strukturované požadavky na hodnocení dodavatelů, smlouvy a monitorování výkonnosti.

11.8.2 BAI03 - Řízení tvorby řešení: přímo se vztahuje k procesům bezpečného SDLC, přezkumům kódování a ověřování vývoje.

11.8.3 DSS05 - Řízení bezpečnostních služeb: je v souladu s monitorováním a ochranou systémů vyvíjených externě nebo třetími stranami.