					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P28					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	Kapitola 8.1	N/A
ISO/IEC 27002:2022	Kontroly 5.19 – 5.22, 8	N/A
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-10	N/A
Nariadenie EÚ GDPR	Články 28, 32	N/A
Smernica EÚ NIS2	Články 21(2)(a), (h), 23	N/A
Nariadenie EÚ DORA	Články 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Účel

1.1 Táto politika stanovuje povinné kontroly pre outsourcing vývoja softvéru alebo systémov externým dodávateľom, zmluvným pracovníkom alebo agentúram s cieľom zabezpečiť, aby boli bezpečné postupy začlenené do celého životného cyklu vývoja.

1.2 Jej cieľom je predchádzať zraniteľnostiam, úniku údajov, ohrozeniu duševného vlastníctva (IP) a porušeniam súladu vyplývajúcim zo zapojenia externých vývojových subjektov.

1.3 Politika stanovuje požiadavky na riadenie dodávateľov, štandardy bezpečného programovania, riadenie prístupu, monitorovanie a ukončenie prístupu po skončení zmluvy s cieľom zachovať dôvernosť, integritu a dostupnosť vyvíjaného softvéru.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky organizačné jednotky, ktoré zapájajú externé subjekty do vývoja softvéru alebo systémov, vrátane:

2.1.1 webových aplikácií, mobilných aplikácií, vstavaných systémov, rozhraní API, skriptov, automatizovaných pracovných postupov alebo modulov platforiem,

2.1.2 zákazkového vývoja pre interné platformy, systémy orientované na klienta alebo komerčné produkty,

2.1.3 spolupráce s externými vývojármi, freelancermi, agentúrami alebo offshore tímami.

2.2 Táto politika upravuje aj činnosť každého externého subjektu, ktorý počas vývoja pristupuje k zdrojovému kódu, testovacím prostrediam alebo CI/CD pipeline.

2.3 Tieto požiadavky sú záväzné bez ohľadu na typ zmluvy, metodiku vývoja alebo geografickú polohu outsourcovaného poskytovateľa.

3. Ciele

3.1 Uplatňovať postupy bezpečného životného cyklu vývoja softvéru (SDLC) vo všetkých outsourcovaných spoluprácach od plánovania až po validáciu po nasadení.

3.2 Zabezpečiť, aby všetky zmluvy s externými vývojármi obsahovali povinné ustanovenia týkajúce sa ochrany údajov, bezpečného programovania a zachovania vlastníctva IP.

3.3 Stanoviť požiadavky na riadenie prístupu, monitorovanie a audit pre vývojárov tretích strán, ktorí pracujú s internými systémami.

3.4 Chrániť organizáciu pred hrozbami v dodávateľskom reťazci, porušeniami právnych predpisov a reputačnou ujmou súvisiacou so softvérom vyvíjaným externe.

3.5 Udržiavať nepretržitý súlad s bezpečnostnými rámcami vrátane ISO/IEC 27001, NIST, GDPR, NIS2, DORA a COBIT 2019.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje vysoko rizikové projekty outsourcovaného vývoja a odôvodnené výnimky z tejto politiky.

4.1.2 Zabezpečuje, aby rozhodnutia o outsourcingu boli v súlade so strategickými cieľmi a apetítom organizácie na riziko.

4.2 Riaditeľ informačnej bezpečnosti (CISO)

4.2.1 Schvaľuje zapojenie dodávateľa z pohľadu informačnej bezpečnosti.

4.2.2 Definuje požiadavky na bezpečnostné kontroly pre outsourcované spolupráce a preskúmava hlásenia incidentov.

[... 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 sa musí preskúmať najmenej raz ročne alebo častejšie za týchto okolností:

9.1.1 zavedenie nových modelov outsourcingu vývoja, dodávateľov alebo jurisdikcií,

9.1.2 aktualizácie regulačných rámcov, ako sú GDPR, NIS2 alebo DORA,

9.1.3 po bezpečnostnom incidente týkajúcom sa outsourcovaného kódu, prístupu alebo výstupov,

9.1.4 ako súčasť auditných zistení alebo zlepšovania ISMS.

9.2 Riaditeľ informačnej bezpečnosti (CISO) je zodpovedný za iniciovanie a koordináciu preskúmania politiky po konzultácii s:

9.2.1.1 právnym oddelením a obstarávaním (pre súlad zmluvného zabezpečenia),

9.2.1.2 vlastníkmi projektov a produktov (pre prevádzkovú realizovateľnosť),

9.2.1.3 Tímom informačnej bezpečnosti (pre aktualizácie hrozieb a kontrol),

9.2.1.4 vrcholovým manažmentom (na konečné schválenie).

9.3 Všetky aktualizácie politiky musia byť:

9.3.1.1 riadené verziami a uložené v určenom úložisku dokumentov,

9.3.1.2 oznámené zainteresovaným stranám zapojeným do činností outsourcovaného vývoja,

9.3.1.3 prepojené s každou aktualizáciou súvisiacich politík alebo procesnej dokumentácie.

9.4 Každú verziu politiky musí sprevádzať zoznam zmien na zabezpečenie sledovateľnosti zmien a schválení.

10. Súvisiace politiky a väzby

10.1 Táto politika podporuje nasledujúce súvisiace dokumenty a je nimi podporovaná:

10.1.1 P1 - Politika informačnej bezpečnosti: Stanovuje bezpečnostné princípy na úrovni organizácie, ktoré sa uplatňujú v internom aj externom vývoji.

10.1.2 P5 - Politika riadenia zmien: Zabezpečuje, aby všetky zmeny súvisiace s nasadením z outsourcovaných kódových základní boli pred implementáciou preskúmané a schválené.

10.1.3 P13 - Politika klasifikácie a označovania údajov: Určuje, ako sa identifikujú citlivé údaje pred ich sprístupnením dodávateľom vývoja alebo repozitárom.

10.1.4 P18 - Politika kryptografických kontrol: Usmerňuje, ako sa musia počas vývoja a dodania spracúvať kľúče, tajomstvá a citlivé prístupové údaje.

10.1.5 P24 - Politika bezpečného vývoja: Definuje základné požiadavky na interné a externé postupy vývoja softvéru.

10.1.6 P30 - Politika reakcie na incidenty: Upravuje, ako sa eskalujú, vyšetrujú a riešia porušenia ochrany údajov alebo bezpečnostné incidenty súvisiace s outsourcovaným vývojom.

10.1.7 P33 - Politika monitorovania auditu a súladu: Stanovuje požiadavky na preskúmanie činností outsourcovaného vývoja počas auditov alebo preskúmaní súladu.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými bezpečnostnými rámcami a predpismi s cieľom zabezpečiť bezpečný outsourcing vývoja softvéru a postupy riadenia dodávateľov.

11.2 ISO/IEC 27001

11.2.1 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: Stanovuje procesné kontroly pre bezpečný vývoj a dodávky tretích strán.

11.3 ISO/IEC 27002:2022 – Kontroly 5.19 až 5.21, 8

11.3.1 Príloha A Kontrola 5.19 – Riadenie vzťahov s dodávateľmi: Vyžaduje formálne dohody s ustanoveniami o bezpečnosti a súlade.

11.3.2 Príloha A Kontrola 5.20 – Riešenie informačnej bezpečnosti v dohodách s dodávateľmi: Zabezpečuje, aby boli do zmlúv zahrnuté kontroly špecifické pre vývoj.

11.3.3 Príloha A Kontrola 5.21 – Riadenie poskytovania služieb dodávateľov: Zahŕňa monitorovanie výstupov a rizík vývoja tretích strán.

11.3.4 Príloha A Kontrola 8.27 – Outsourcovaný vývoj: Vyžaduje definované bezpečnostné požiadavky a riadenie prístupu k softvéru vyvíjanému externe.

11.3.5 Tieto kontroly stanovujú štruktúrované požiadavky na výber, zazmluvnenie a dohľad nad externými vývojármi vrátane praktík bezpečného vývoja, nakladania s kódom a validácie výkonnosti.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SA-4 – Proces obstarávania: Vyžaduje, aby boli požiadavky bezpečného vývoja definované už v čase obstarávania.

11.4.2 SA-9 – Služby externých systémov: Upravuje, ako majú vývojári tretích strán bezpečne pracovať s internými službami.

11.4.3 SA-10 – Riadenie konfigurácie vývojára: Je v súlade s povinnosťami externých tímov v oblasti riadenia verzií, prístupu ku kódu a sledovania zmien.

11.5 Nariadenie EÚ GDPR (2016/679)

11.5.1 Článok 28 – Povinnosti sprostredkovateľa: Vyžaduje, aby zmluvy s externými vývojármi špecifikovali bezpečnostné, kontrolné a auditné požiadavky pri nakladaní s osobnými údajmi.

11.5.2 Článok 32 – Bezpečnosť spracúvania: Vyžaduje primerané ochranné opatrenia (napr. šifrovanie, riadenie prístupu) pri vývoji systémov, ktoré spracúvajú osobné údaje.

11.6 Smernica EÚ NIS2 (2022/2555)

11.6.1 Články 21(2)(a), (h), 23: Vyžadujú uplatňovanie bezpečných vývojových postupov v spolupráci s tretími stranami a v digitálnych dodávateľských reťazcoch vrátane dohľadu a technického overovania.

11.7 Nariadenie EÚ DORA (2022/2554)

11.7.1 Články 28(1), (2): Vyžadujú, aby finančné subjekty riadili riziko tretích strán v oblasti IKT prostredníctvom zmluvných kontrol a dohľadu nad bezpečným vývojom, najmä pri kritickom outsourcovanom vývoji.

11.8 COBIT 2019

11.8.1 APO10 – Riadenie dodávateľov: Stanovuje štruktúrované požiadavky na hodnotenie dodávateľov, zmluvy a monitorovanie výkonnosti.

11.8.2 BAI03 – Riadenie tvorby riešení: Priamo sa vzťahuje na procesy bezpečného SDLC, preskúmania kódu a validáciu vývoja.

11.8.3 DSS05 – Riadenie bezpečnostných služieb: Je v súlade s monitorovaním a ochranou systémov vyvíjaných externe alebo tretími stranami.