					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P25S					Názov dokumentu: **Politika požiadaviek na bezpečnosť aplikácií**							
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	Prevádzkové kontroly vrátane bezpečnosti aplikácií
ISO/IEC 27002:2022	Kontroly 8.25 – 8.26	Bezpečný návrh, vývoj, testovanie a preskúmanie kódu
NIST SP 800-53 Rev.5	SA-11, SI-10	Testovanie vývojármi/aplikácií, analýza kódu, prevencia chýb
GDPR EÚ	Článok 25	Ochrana súkromia už pri návrhu a štandardne
Smernica EÚ NIS2	Článok 21(2)(a), (e)	Technické opatrenia na zabezpečenie aplikácií a detekciu rizík
Nariadenie EÚ DORA	Články 9(2)(c), 10(2)(c)	Bezpečnosť aplikácií na zabezpečenie digitálnej prevádzkovej odolnosti
COBIT 2019	BAI03	Riadenie identifikácie riešení a vývoja/obstarania bezpečného softvéru

1. Účel

1.1 Táto politika stanovuje minimálne povinné kontroly bezpečnosti aplikácií vyžadované pre všetky softvérové a systémové riešenia používané organizáciou bez ohľadu na to, či sú vyvíjané interne alebo obstarávané od externých dodávateľov.

1.2 Zabezpečuje, aby boli aplikácie navrhované, implementované a udržiavané tak, aby chránili údaje zákazníkov, zamestnancov a informácie organizácie pred neoprávneným prístupom, zneužitím, zmenou alebo zničením.

1.3 Táto politika podporuje úsilie organizácie o získanie a udržanie certifikácie ISO/IEC 27001, plnenie povinností podľa GDPR a NIS2 a znižovanie prevádzkových rizík spojených s nebezpečným nasadzovaním softvéru.

1.4 Pomáha vytvoriť konzistentný a overiteľný prístup k bezpečnosti aplikácií pre MSP stanovením jednotného kontrolného zoznamu bezpečnostných funkcií a postupov prispôsobeného prostrediam s obmedzenými internými technickými zdrojmi.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky aplikácie, systémy, nástroje a platformy, ktoré:

2.1.1 sú vyvíjané interne, prispôsobované alebo skriptované na interné použitie,

2.1.2 sú obstarávané ako komerčný softvér, SaaS alebo systémy v cloudovom prostredí,

2.1.3 spracúvajú, uchovávajú alebo prenášajú osobné údaje, prevádzkové záznamy alebo citlivé prevádzkové informácie,

2.1.4 sú prístupné zamestnancom, zmluvným pracovníkom, zákazníkom alebo partnerom prostredníctvom interných sietí, internetu alebo mobilných platforiem.

2.2 Politika sa vzťahuje na:

2.2.1 vývojárov (interných alebo zmluvných),

2.2.2 dodávateľov softvéru a poskytovateľov cloudových služieb,

2.2.3 pracovníkov IT podpory alebo administrátorov zodpovedných za nasadenie a podporu,

2.2.4 vlastníkov aplikácií a biznis používateľov zapojených do schvaľovania a dohľadu nad systémami.

3. Ciele

3.1 Zabezpečiť, aby všetky aplikácie používané organizáciou obsahovali zabudované a overiteľné bezpečnostné kontroly, ktoré zmierňujú bežné softvérové zraniteľnosti.

3.2 Chrániť dôvernosť, integritu a dostupnosť údajov spracúvaných aplikáciami bez ohľadu na to, kde sú hostované.

3.3 Vyžadovať formálne testovanie, preskúmanie a validáciu bezpečnosti aplikácií pred schválením akejkoľvek novej aplikácie alebo významnej aktualizácie na používanie v produkčnom prostredí.

3.4 Umožniť konzistentné a bezpečné nakladanie s prihlasovacími údajmi používateľov, údajmi relácií a prístupovými právami vo všetkých kriticky dôležitých systémoch.

3.5 Vyžadovať bezpečné auditné logovanie, auditovateľnosť a monitorovacie funkcie vo všetkých aplikáciách na podporu detekcie podozrivej aktivity a reakcie na ňu.

3.6 Znižovať právne a compliance riziká tým, že aplikácie budú spĺňať príslušné regulačné bezpečnostné požiadavky.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Nesie celkovú zodpovednosť za bezpečnosť aplikácií v celej organizácii.

4.1.2 Schvaľuje túto politiku a zabezpečuje, aby všetky obstarávania alebo vývojové projekty boli s ňou v súlade.

4.1.3 Zabezpečuje, aby dodávatelia a poskytovatelia služieb boli zmluvne viazaní požiadavkami na bezpečnosť aplikácií.

4.1.4 Preskúmava a schvaľuje výnimky z rizika, ak z dôvodu prevádzkových obmedzení nemožno dosiahnuť úplný súlad.

4.2 Vlastník aplikácie (ak je určený)

4.2.1 Identifikuje bezpečnostné potreby konkrétnej aplikácie počas výberu systému alebo pri začatí projektu.

4.2.2 Overuje, že sú zahrnuté kľúčové funkcie, ako ochrana prihlásenia, šifrovanie a protokolovanie aktivít.

4.2.3 Zúčastňuje sa preskúmaní pred nasadením a potvrdzuje, že bezpečnostné kontroly zodpovedajú prevádzkovým potrebám.

[... 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 za kalendárny rok s cieľom:

9.1.1 zohľadniť zmeny regulačných požiadaviek (napr. GDPR, NIS2, DORA),

9.1.2 zapracovať nové alebo vznikajúce hrozby a techniky útokov,

9.1.3 aktualizovať znenie a požiadavky tak, aby odrážali zmeny platforiem, dodávateľov alebo metód vývoja.

9.2 Priebežné preskúmania sa musia vykonať aj vtedy, keď:

9.2.1 sa zavádzajú nové aplikácie,

9.2.2 existujúce aplikácie prechádzajú významnými aktualizáciami alebo integráciou,

9.2.3 dôjde k incidentu alebo porušeniu ochrany údajov súvisiacemu s aplikáciou,

9.2.4 sú identifikované nové riziká na základe externých upozornení alebo odvetvových výstrah.

9.3 Všetky aktualizácie tejto politiky musia byť:

9.3.1 schválené Generálnym manažérom,

9.3.2 zdokumentované s históriou verzií a dôvodom zmeny,

9.3.3 oznámené všetkým zamestnancom, vývojárom a dodávateľom zapojeným do správy aplikácií,

9.3.4 bezpečne uchovávané na účely auditu a preukazovania súladu.

10. Súvisiace politiky a väzby

10.1 Táto politika je priamo podporovaná nasledujúcimi bezpečnostnými politikami zosúladenými pre MSP a prispieva k ich uplatňovaniu:

10.1.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: určuje zodpovednosť za schvaľovanie aplikácií, uplatňovanie politiky a riadenie dodávateľov.

10.1.2 P4S – Politika riadenia prístupu: zabezpečuje, aby prístup k aplikáciám bol v súlade so zásadou minimálnych oprávnení a zásadami správy relácií.

10.1.3 P8S – Politika povedomia a školenia v oblasti informačnej bezpečnosti: zabezpečuje, aby boli používatelia a vývojári školení v rozpoznávaní a nahlasovaní hrozieb súvisiacich s aplikáciami.

10.1.4 P17S – Politika ochrany údajov a súkromia: poskytuje ochranné opatrenia na ochranu údajov, ktoré musí uplatňovať každá aplikácia spracúvajúca osobné informácie.

10.1.5 P14S – Politika uchovávania a likvidácie údajov: upravuje, ako sa musia logy, zálohy a citlivé údaje vytvorené aplikáciou uchovávať, archivovať a bezpečne likvidovať.

10.1.6 P30S – Politika reakcie na incidenty: stanovuje kroky na identifikáciu, nahlasovanie a zamedzenie šírenia bezpečnostných udalostí súvisiacich s aplikáciami.

10.2 Tieto politiky spolu zabezpečujú, že bezpečnosť aplikácií je plne integrovaná do systému manažérstva informačnej bezpečnosti (ISMS) organizácie a podporuje pripravenosť na audit.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje, aby organizácie zaviedli prevádzkové kontroly na riešenie rizík informačnej bezpečnosti vrátane rizík súvisiacich s aplikáciami a softvérovými systémami.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.25 – Odporúča implementovať postupy bezpečného návrhu, vývoja a preskúmania kódu vo všetkých aplikáciách vrátane aplikácií poskytovaných dodávateľmi.

11.2.2 Kontrola 8.26 – Odporúča formálne testovanie kontrol bezpečnosti aplikácií, najmä v oblastiach riadenia prístupu, validácie vstupov a správy relácií.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Špecifikuje požiadavky na testovanie vývojármi, analýzu kódu a dynamické skenovanie aplikácií pred nasadením.

11.3.2 SI-10 – Zameriava sa na detekciu a prevenciu bežných softvérových chýb s dôrazom na povedomie vývojárov a technické ochranné opatrenia.

11.4 GDPR EÚ (2016/679)

11.4.1 Článok 25 – „Ochrana súkromia už pri návrhu a štandardne“ vyžaduje zabudovanie ochrany súkromia a bezpečnosti do základného návrhu aplikácií spracúvajúcich osobné údaje.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(a) a (e) – Vyžaduje, aby základné a dôležité subjekty zaviedli technické opatrenia na zabezpečenie aplikácií a detekciu rizík súvisiacich so softvérom.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 9(2)(c), 10(2)(c) – Vyžaduje, aby MSP vo finančnom sektore zaviedli bezpečnostné kontroly na úrovni aplikácií a vykonávali pravidelné posúdenia na udržanie digitálnej prevádzkovej odolnosti.

11.7 COBIT 2019

11.7.1 BAI03 – „Riadenie identifikácie riešení a tvorby“ usmerňuje vývoj alebo obstaranie bezpečného softvéru zosúladeného s rizikami, požiadavkami na súlad a požiadavkami organizácie aj v prostredí MSP s obmedzenými zdrojmi.