					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P25					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	—
ISO/IEC 27002:2022	Kontroly 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
Nariadenie EÚ GDPR	Články 25, 32	—
Smernica EÚ NIS2	Články 21(2)(f), 23	—
Nariadenie EÚ DORA	Články 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Účel

1.1 Táto politika stanovuje záväzné požiadavky na bezpečnosť aplikačnej vrstvy pre softvér vyvíjaný, obstarávaný, integrovaný alebo nasadzovaný organizáciou. Zabezpečuje, aby boli všetky aplikácie navrhované, implementované a udržiavané v súlade s princípmi bezpečného vývoja, regulačnými povinnosťami a apetítom organizácie na riziko.

1.2 Táto politika vyžaduje začlenenie bezpečnosti do celého životného cyklu aplikácie vrátane autentifikácie používateľov, spracúvania údajov, ochrany rozhraní a bezpečnej interakcie s API a službami.

1.3 Prijatím tejto politiky organizácia sleduje cieľ predchádzať vzniku softvérových zraniteľností, chrániť citlivé údaje a zabezpečiť sledovateľnosť a odolnosť voči zneužitiu a neoprávnenému používaniu.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky:

2.1.1 interne vyvíjané alebo externe obstarávané aplikácie vrátane SaaS a riešení vyvíjaných na mieru,

2.1.2 aplikácie podporujúce kritické prevádzkové činnosti, prístup zákazníkov alebo spracúvanie regulovaných údajov,

2.1.3 tímy vývoja, DevOps, QA, produktové a bezpečnostné tímy,

2.1.4 externých vývojárov, dodávateľov softvéru a integračných partnerov s prístupom k aplikáciám organizácie alebo k API.

2.2 Vzťahuje sa na všetky prostredia: vývojové, testovacie, staging, produkčné a prostredie obnovy po havárii bez ohľadu na to, či sú prevádzkované vo vlastných priestoroch, v súkromných dátových centrách alebo vo verejných cloudových prostrediach.

3. Ciele

3.1 Definovať základné funkčné a nefunkčné bezpečnostné požiadavky, ktoré musia spĺňať všetky aplikácie bez ohľadu na metodiku vývoja alebo technologický stack.

3.2 Zabezpečiť integráciu ochranných opatrení na aplikačnej vrstve vrátane validácie vstupov, kódovania výstupov, spracovania chýb a zabezpečenia relácií.

3.3 Vyžadovať bezpečnú implementáciu mechanizmov autentifikácie, autorizácie a riadenia prístupu v súlade s politikami organizácie pre identitu a prístup.

3.4 Stanoviť povinnosť bezpečnej interakcie s API, webovými rozhraniami a komponentmi tretích strán s použitím schválených protokolov a bezpečnostných kontrol.

3.5 Umožniť včasnú detekciu a zmierňovanie zraniteľností prostredníctvom statickej a dynamickej analýzy, preskúmania kódu a modelovania hrozieb.

3.6 Chrániť citlivé údaje v súlade s regulačnými požiadavkami prostredníctvom uplatňovania šifrovania, klasifikácie a pravidiel uchovávania údajov.

3.7 Zabezpečiť nepretržitú validáciu bezpečnostného stavu aplikácií po nasadení prostredníctvom testovania, monitorovania a pripravenosti na audit.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje jej súlad so stratégiou informačnej bezpečnosti organizácie a jej rizikovým profilom.

4.1.2 Schvaľuje požiadavky na bezpečnosť aplikácií a presadzuje povinné kontroly v oblasti vývoja a obstarávania.

4.2 vedúci bezpečnosti aplikácií / manažér DevSecOps

4.2.1 Definuje základný súbor bezpečnostných kontrol a metodík testovania pre aplikačné komponenty.

4.2.2 Dohliada na bezpečnú integráciu nástrojov, ako sú SAST, DAST, IAST a SCA, do pipeline dodávky softvéru.

4.2.3 Udržiava kontrolný zoznam požiadaviek na bezpečnosť aplikácií a validačné kritériá.

[... 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 musí byť preskúmaná najmenej raz ročne alebo častejšie v reakcii na:

9.1.1 zverejnenie kritických zraniteľností ovplyvňujúcich bežne používané frameworky alebo závislosti,

9.1.2 aktualizácie regulačných povinností v oblasti bezpečnosti aplikácií (napr. NIS2, DORA),

9.1.3 významné zmeny v postupoch vývoja softvéru, nástrojoch alebo cloudovej architektúre organizácie,

9.1.4 zistenia z interných auditov alebo externých penetračných testov.

9.2 Preskúmanie vedie vedúci bezpečnosti aplikácií v koordinácii s CISO, vedúcimi DevOps inžinierstva, právneho oddelenia, obstarávania a QA.

9.3 Všetky revízie musia podliehať riadeniu verzií v registri riadenej dokumentácie ISMS a musia byť distribuované všetkým dotknutým vývojovým a produktovým tímom.

9.4 Nahradené verzie musia byť archivované najmenej tri roky na účely sledovateľnosti, auditovateľnosti a podpory vyšetrovania porušenia ochrany údajov.

10. Súvisiace politiky a väzby

10.1 P1 – Politika informačnej bezpečnosti. Stanovuje základ ochrany systémov a údajov, na základe ktorého sa vyžadujú kontroly na aplikačnej úrovni na predchádzanie neoprávnenému prístupu, únikom údajov a zneužitiu.

10.2 P4 – Politika riadenia prístupu. Definuje štandardy riadenia identít a relácií, ktoré musia uplatňovať všetky aplikácie vrátane silnej autentifikácie, zásady minimálnych oprávnení a požiadaviek na revíziu prístupových práv.

10.3 P5 – Politika riadenia zmien. Upravuje presun aplikačného kódu a konfigurácií do produkčných prostredí a zabezpečuje blokovanie neautorizovaných alebo netestovaných zmien.

10.4 P17 – Politika ochrany údajov a súkromia. Vyžaduje, aby aplikácie uplatňovali ochranu súkromia už pri návrhu a štandardne a zabezpečovali zákonné spracúvanie, šifrovanie a uchovávanie osobných a citlivých údajov vo všetkých prostrediach.

10.5 P24 – Politika bezpečného vývoja. Poskytuje širší rámec na začlenenie bezpečnosti do životného cyklu vývoja softvéru, pričom táto politika stanovuje konkrétne požiadavky a technické kontroly, ktoré sa majú implementovať na aplikačnej vrstve.

10.6 P30 – Politika reakcie na incidenty. Stanovuje povinnosť štruktúrovaného riešenia bezpečnostných incidentov aplikácií vrátane zraniteľností identifikovaných po nasadení alebo počas penetračného testovania a určuje postupy eskalácie, zamedzenia šírenia a obnovy.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001:2022

11.1.1 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: Vyžaduje začlenenie bezpečnosti aplikácií do procesov a systémov s cieľom zabezpečiť dôvernosť, integritu a dostupnosť.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroly 8.25–8.26: Podrobnejšie určujú očakávania pre bezpečnosť aplikačnej vrstvy vrátane postupov bezpečného kódovania, modelovania hrozieb, architektonických kontrol a validácie softvéru tretích strán.

11.2.2 Príloha A, kontrola 8.25 – Životný cyklus bezpečného vývoja: Vyžaduje integráciu bezpečnosti v celom životnom cykle aplikácie.

11.2.3 Príloha A, kontrola 8.26 – Požiadavky na bezpečnosť aplikácií: Stanovuje povinnosť definovať a uplatňovať technické kontroly na ochranu aplikácií pred zneužitím a kompromitáciou.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Bezpečnostné testovanie a hodnotenie vývojárom: Vyžaduje statické, dynamické a penetračné testovanie počas vývoja.

11.3.2 SA-15 – Proces vývoja, štandardy a nástroje: Zavádza formálne štandardy pre bezpečný vývoj aplikácií.

11.3.3 SI-10 – Validácia vstupných informácií: Vyžaduje kontrolné mechanizmy na predchádzanie útokom typu injection a útokom na parsovanie.

11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 25 – Ochrana údajov už pri návrhu a štandardne: Vyžaduje integráciu ochrany údajov a súkromia do aplikačnej logiky a pracovných postupov.

11.4.2 Článok 32 – Bezpečnosť spracúvania: Stanovuje povinnosť primeraných technických opatrení, ako sú validácia vstupov, šifrovanie a bezpečné kontroly prístupu.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(f): Vyžaduje riešenie zraniteľností a uplatňovanie postupov bezpečného životného cyklu aplikácií pre základné a dôležité subjekty.

11.5.2 Článok 23 – Nahlasovanie bezpečnostných incidentov: Vyžaduje schopnosti logovania a monitorovania na aplikačnej vrstve na detekciu a nahlasovanie významných incidentov.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 9 – Riadenie rizík IKT: Ukladá finančným subjektom povinnosť zabezpečiť, aby boli aplikácie bezpečné, testované a odolné voči kybernetickým hrozbám.

11.6.2 Článok 11 – Testovanie nástrojov IKT: Podporuje pravidelné penetračné testovanie a cvičenia red teamu pre kritické aplikácie a služby.

11.7 COBIT 2019

11.7.1 BAI03 – Riadenie identifikácie a tvorby riešení: Stanovuje požiadavky na návrh a kontroly počas vývoja aplikácií.

11.7.2 BAI09 – Riadenie aplikácií: Zdôrazňuje bezpečnú údržbu, monitorovanie a rozvoj prevádzkovaných aplikácií.

11.7.3 DSS05 – Riadenie bezpečnostných služieb: Prepája ochranu aplikácií so širšími bezpečnostnými operáciami a kontrolami organizácie.