					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P25					Název dokumentu: **Politika požadavků na zabezpečení aplikací**							
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	—
ISO/IEC 27002:2022	Opatření 8.25–8.28	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
GDPR EU	Články 25, 32	—
směrnice EU NIS2	Články 21(2)(f), 23	—
nařízení EU DORA	Články 9, 11	—
COBIT 2019	BAI03, BAI09, DSS	—

1. Účel

1.1 Tato politika stanoví závazné požadavky na zabezpečení aplikací pro software vyvíjený, pořizovaný, integrovaný nebo nasazovaný organizací. Zajišťuje, aby všechny aplikace byly navrhovány, implementovány a udržovány v souladu se zásadami bezpečného vývoje, regulatorními požadavky a apetitem organizace k riziku.

1.2 Tato politika vyžaduje začlenění bezpečnosti do celého životního cyklu aplikace, včetně autentizace uživatelů, nakládání s daty, ochrany rozhraní a bezpečné interakce s API a službami.

1.3 Přijetím této politiky organizace usiluje o prevenci zavádění zranitelností do softwaru, ochranu citlivých dat a zajištění dohledatelnosti a odolnosti vůči zneužití a narušení.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 interně vyvíjené nebo externě pořizované aplikace, včetně SaaS a nástrojů vyvíjených na míru,

2.1.2 aplikace podporující kritické podnikové činnosti, přístup zákazníků nebo zpracování regulovaných dat,

2.1.3 týmy vývoje, DevOps, QA, produktové týmy a bezpečnostní týmy,

2.1.4 externí vývojáře, dodavatele softwaru a integrační partnery s přístupem k aplikacím organizace nebo k API.

2.2 Vztahuje se na všechna prostředí: vývojové, testovací, předprodukční, produkční a prostředí pro obnovu po havárii, bez ohledu na to, zda jsou provozována on-premise, v privátních datových centrech nebo ve veřejných cloudových prostředích.

3. Cíle

3.1 Stanovit základní funkční a nefunkční bezpečnostní požadavky, které musí splňovat všechny aplikace bez ohledu na způsob vývoje nebo technologický stack.

3.2 Zajistit implementaci bezpečnostních opatření na aplikační vrstvě, včetně validace vstupů, kódování výstupů, ošetření chyb a zabezpečení relací.

3.3 Vyžadovat bezpečnou implementaci mechanismů autentizace, autorizace a řízení přístupu v souladu s politikami organizace pro řízení identit a přístupů.

3.4 Stanovit povinnost bezpečné interakce s API, webovými rozhraními a komponentami třetích stran za použití schválených protokolů a bezpečnostních opatření.

3.5 Umožnit včasnou detekci a zmírňování zranitelností prostřednictvím statické a dynamické analýzy, přezkumů kódu a modelování hrozeb.

3.6 Chránit citlivá data v souladu s regulatorními požadavky prostřednictvím vynucování šifrování, klasifikace a pravidel uchovávání dat.

3.7 Zajistit průběžné ověřování bezpečnostního stavu aplikací po nasazení prostřednictvím testování, monitorování a připravenosti na audit.

4. Role a odpovědnosti

4.1 Ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za tuto politiku a zajišťuje její soulad se strategií informační bezpečnosti a apetitem organizace k riziku.

4.1.2 Schvaluje požadavky na zabezpečení aplikací a prosazuje závazná opatření napříč vývojem a pořizováním.

4.2 Vedoucí zabezpečení aplikací / manažer DevSecOps

4.2.1 Stanovuje základní bezpečnostní opatření a metodiky testování pro aplikační komponenty.

4.2.2 Zajišťuje bezpečnou integraci nástrojů, jako jsou SAST, DAST, IAST a SCA, do pipeline dodávky softwaru.

4.2.3 Udržuje kontrolní seznam požadavků na zabezpečení aplikací a validační kritéria.

[... 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 přezkoumávána každoročně nebo častěji v reakci na:

9.1.1 zveřejnění kritických zranitelností ovlivňujících běžně používané frameworky nebo závislosti,

9.1.2 aktualizace regulatorních povinností v oblasti zabezpečení aplikací (např. NIS2, DORA),

9.1.3 významné změny v postupech vývoje softwaru, nástrojích nebo cloudové architektuře organizace,

9.1.4 zjištění z interních auditů nebo externích penetračních testů.

9.2 Přezkum vede Vedoucí zabezpečení aplikací v koordinaci s CISO, vedoucími DevOps Engineeringu, právním oddělením, compliance, pořizováním a QA.

9.3 Všechny revize musí být vedeny v režimu správy verzí v registru řízení dokumentace ISMS a distribuovány všem dotčeným vývojovým a produktovým týmům.

9.4 Nahrazené verze musí být archivovány po dobu nejméně tří let za účelem zajištění dohledatelnosti, auditovatelnosti a podpory vyšetřování případů porušení bezpečnosti dat.

10. Související politiky a vazby

10.1 P1 – Politika informační bezpečnosti. Stanoví základ pro ochranu systémů a dat, v jehož rámci jsou vyžadována opatření na aplikační úrovni k prevenci neoprávněného přístupu, úniku dat a zneužití.

10.2 P4 – Politika řízení přístupu. Definuje standardy pro řízení identit a relací, které musí uplatňovat všechny aplikace, včetně silné autentizace, zásady minimálních oprávnění a požadavků na přezkum přístupových práv.

10.3 P5 – Politika řízení změn. Upravuje přesun aplikačního kódu a konfigurací do produkčních prostředí a zajišťuje, aby neoprávněné nebo netestované změny byly blokovány.

10.4 P17 – Politika ochrany dat a soukromí. Vyžaduje, aby aplikace uplatňovaly ochranu osobních údajů již od návrhu a zajišťovaly zákonné nakládání s osobními a citlivými daty, jejich šifrování a uchovávání ve všech prostředích.

10.5 P24 – Politika bezpečného vývoje. Poskytuje širší rámec pro začlenění bezpečnosti do SDLC, přičemž tato politika stanoví konkrétní požadavky a technická opatření, která mají být implementována na aplikační vrstvě.

10.6 P30 – Politika reakce na incidenty (P30). Vyžaduje strukturované zvládání incidentů zabezpečení aplikací, včetně zranitelností identifikovaných po nasazení nebo během penetračního testování, a stanoví postupy eskalace, omezení dopadu a obnovy.

11. Referenční normy a rámce

11.1 ISO/IEC 27001:2022

11.1.1 Kapitola 8.1 – Provozní plánování a řízení: Vyžaduje, aby zabezpečení aplikací bylo začleněno do procesů a systémů za účelem zajištění důvěrnosti, integrity a dostupnosti.

11.2 ISO/IEC 27002:2022

11.2.1 Opatření 8.25–8.26: Upřesňují očekávání pro zabezpečení aplikací, včetně postupů bezpečného kódování, modelování hrozeb, architektonických opatření a validace softwaru třetích stran.

11.2.2 Příloha A, opatření 8.25 – Životní cyklus bezpečného vývoje: Vyžaduje začlenění bezpečnosti do celého životního cyklu aplikace.

11.2.3 Příloha A, opatření 8.26 – Požadavky na zabezpečení aplikací: Stanoví povinnost definovat a prosazovat technická opatření na ochranu aplikací proti zneužití a kompromitaci.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Bezpečnostní testování a hodnocení vývojářem: Vyžaduje statické, dynamické a penetrační testování v průběhu vývoje.

11.3.2 SA-15 – Proces vývoje, standardy a nástroje: Stanoví formální standardy pro bezpečný vývoj aplikací.

11.3.3 SI-10 – Validace informačních vstupů: Vyžaduje řídicí mechanismy pro prevenci injekčních útoků a útoků proti parsování.

11.4 GDPR EU (2016/679)

11.4.1 Článek 25 – Ochrana osobních údajů již od návrhu a ve výchozím nastavení: Vyžaduje integraci ochrany dat a soukromí do aplikační logiky a pracovních postupů.

11.4.2 Článek 32 – Zabezpečení zpracování: Vyžaduje přiměřená technická opatření, jako jsou validace vstupů, šifrování a bezpečné řízení přístupu.

11.5 směrnice EU NIS2 (2022/2555)

11.5.1 Článek 21(2)(f): Vyžaduje zvládání zranitelností a postupy bezpečného životního cyklu aplikací pro základní a důležité subjekty.

11.5.2 Článek 23 – Hlášení bezpečnostních incidentů: Vyžaduje schopnosti protokolování a monitorování na aplikační vrstvě pro detekci a hlášení významných incidentů.

11.6 nařízení EU DORA (2022/2554)

11.6.1 Článek 9 – Řízení rizik v oblasti ICT: Ukládá finančním subjektům povinnost zajistit, aby aplikace byly bezpečné, testované a odolné vůči kybernetickým hrozbám.

11.6.2 Článek 11 – Testování nástrojů ICT: Podporuje pravidelné penetrační testování a cvičení red teamu u kritických aplikací a služeb.

11.7 COBIT 2019

11.7.1 BAI03 – Řízení identifikace a tvorby řešení: Stanoví požadavky na návrh a opatření během vývoje aplikací.

11.7.2 BAI09 – Řízení aplikací: Zdůrazňuje bezpečnou údržbu, monitorování a rozvoj provozovaných aplikací.

11.7.3 DSS05 – Řízení bezpečnostních služeb: Propojuje ochranu aplikací s širšími bezpečnostními operacemi a opatřeními organizace.