					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P25S					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	Provozní opatření včetně zabezpečení aplikací
ISO/IEC 27002:2022	Opatření 8.25–8.26	Bezpečný návrh, vývoj, testování a přezkum kódu
NIST SP 800-53 Rev.5	SA-11, SI-10	Testování vývojáři / testování aplikací, analýza kódu, prevence chyb
GDPR EU	Článek 25	Ochrana osobních údajů již od návrhu a ve výchozím nastavení
směrnice EU NIS2	Článek 21 odst. 2 písm. a), e)	Technická opatření k zabezpečení aplikací a detekci rizik
nařízení EU DORA	Články 9 odst. 2 písm. c), 10 odst. 2 písm. c)	Zabezpečení aplikací pro digitální provozní odolnost
COBIT 2019	BAI03	Řízení bezpečného vývoje / pořízení softwaru

1. Účel

1.1 Tato politika stanoví minimální povinná bezpečnostní opatření pro aplikace, která se vyžadují pro veškerý software a systémová řešení používaná organizací bez ohledu na to, zda jsou vyvíjena interně nebo pořizována od externích dodavatelů.

1.2 Zajišťuje, aby byly aplikace navrhovány, implementovány a udržovány způsobem, který chrání údaje zákazníků, zaměstnanců a obchodní údaje před neoprávněným přístupem, zneužitím, změnou nebo zničením.

1.3 Tato politika podporuje úsilí organizace o získání a udržení certifikace ISO/IEC 27001, plnění povinností podle GDPR a NIS2 a snižování provozních rizik souvisejících s nedostatečně zabezpečeným nasazením softwaru.

1.4 Pomáhá vytvořit konzistentní a auditovatelný přístup k zabezpečení aplikací pro SME tím, že stanoví jednotný kontrolní seznam bezpečnostních funkcí a postupů přizpůsobený prostředím s omezenými interními technickými zdroji.

2. Rozsah

2.1 Tato politika se vztahuje na všechny aplikace, systémy, nástroje a platformy, které:

2.1.1 jsou vyvíjeny interně, upravovány na míru nebo skriptovány pro interní použití,

2.1.2 jsou pořizovány jako komerční software, SaaS nebo cloudové systémy,

2.1.3 zpracovávají, ukládají nebo přenášejí osobní údaje, obchodní záznamy nebo citlivé provozní informace,

2.1.4 jsou přístupné zaměstnancům, smluvním pracovníkům, zákazníkům nebo partnerům prostřednictvím interních sítí, internetu nebo mobilních platforem.

2.2 Tato politika se vztahuje na:

2.2.1 vývojáře (interní i smluvní),

2.2.2 dodavatele softwaru a poskytovatele cloudových služeb,

2.2.3 pracovníky IT podpory nebo správce odpovědné za nasazení a podporu,

2.2.4 vlastníky aplikací a podnikové uživatele zapojené do schvalování systémů a dohledu nad nimi.

3. Cíle

3.1 Zajistit, aby všechny aplikace používané organizací obsahovaly zabudovaná a ověřitelná bezpečnostní opatření, která zmírňují běžné zranitelnosti softwaru.

3.2 Chránit důvěrnost, integritu a dostupnost dat zpracovávaných aplikacemi bez ohledu na to, kde jsou hostována.

3.3 Vyžadovat formální testování, přezkum a ověření zabezpečení aplikací před schválením jakékoli nové aplikace nebo významné aktualizace pro použití v produkčním prostředí.

3.4 Umožnit konzistentní a bezpečné nakládání s uživatelskými přihlašovacími údaji, daty relací a přístupovými právy napříč všemi systémy kritickými pro podnikání.

3.5 Vyžadovat bezpečné protokolování, auditovatelnost a monitorovací funkce ve všech aplikacích na podporu detekce podezřelé činnosti a reakce na ni.

3.6 Snižovat právní a compliance rizika tím, že aplikace budou splňovat příslušné regulatorní bezpečnostní požadavky.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Nese celkovou odpovědnost za zabezpečení aplikací v celé organizaci.

4.1.2 Schvaluje tuto politiku a zajišťuje, aby všechny akvizice nebo vývojové projekty byly v souladu s touto politikou.

4.1.3 Zajišťuje, aby dodavatelé a poskytovatelé služeb byli smluvně zavázáni k plnění požadavků na zabezpečení aplikací.

4.1.4 Přezkoumává a schvaluje výjimky z rizik v případech, kdy z důvodu obchodních omezení nelze dosáhnout plného souladu.

4.2 vlastník aplikace (je-li určen)

4.2.1 Identifikuje bezpečnostní potřeby specifické pro aplikaci při výběru systému nebo zahájení projektu.

4.2.2 Ověřuje, že jsou zahrnuty klíčové funkce, jako je ochrana přihlášení, šifrování a protokolování činností.

4.2.3 Účastní se přezkumů před nasazením a potvrzuje, že bezpečnostní opatření odpovídají obchodním potřebám.

[... 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 generálním ředitelem přezkoumána nejméně jednou za kalendářní rok, aby:

9.1.1 odrážela změny regulatorních požadavků (např. GDPR, NIS2, DORA),

9.1.2 zahrnovala nové nebo nově vznikající hrozby a techniky útoků,

9.1.3 aktualizovala formulace a požadavky s ohledem na změny platforem, dodavatelů nebo metod vývoje.

9.2 Mimořádné přezkumy musí být provedeny také v případě, že:

9.2.1 jsou zaváděny nové aplikace,

9.2.2 stávající aplikace procházejí významnými aktualizacemi nebo integrací,

9.2.3 dojde k incidentu nebo narušení bezpečnosti souvisejícímu s aplikací,

9.2.4 jsou identifikována nová rizika na základě externích upozornění nebo oborových varování.

9.3 Všechny aktualizace této politiky musí být:

9.3.1 schváleny generálním ředitelem,

9.3.2 zdokumentovány s historií verzí a důvodem změny,

9.3.3 oznámeny všem zaměstnancům, vývojářům a dodavatelům zapojeným do správy aplikací,

9.3.4 bezpečně uloženy pro potřeby auditu a doložení souladu.

10. Související politiky a vazby

10.1 Tato politika je přímo podporována následujícími bezpečnostními politikami sladěnými pro SME a přispívá k jejich uplatňování:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: stanoví odpovědnost za schvalování aplikací, uplatňování politiky a řízení dodavatelů.

10.1.2 P4S – Politika řízení přístupu: zajišťuje, aby přístup k aplikacím odpovídal zásadě minimálních oprávnění a principům řízení relací.

10.1.3 P8S – Politika povědomí o bezpečnosti informací a školení: zajišťuje, aby byli uživatelé a vývojáři školeni v rozpoznávání a hlášení hrozeb souvisejících s aplikacemi.

10.1.4 P17S – Politika ochrany dat a soukromí: poskytuje opatření na ochranu soukromí, která musí uplatňovat každá aplikace zpracovávající osobní údaje.

10.1.5 P14S – Politika uchovávání údajů: upravuje, jak musí být logy vytvářené aplikacemi, zálohy a citlivá data uchovávány, archivovány a bezpečně likvidovány.

10.1.6 P30S – Politika reakce na incidenty: stanoví kroky pro identifikaci, hlášení a zamezení šíření bezpečnostních událostí souvisejících s aplikacemi.

10.2 Tyto politiky společně zajišťují, že zabezpečení aplikací je plně integrováno do systému řízení bezpečnosti informací (ISMS) organizace a že organizace je připravena na audit.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje, aby organizace zavedly provozní opatření k řešení rizik bezpečnosti informací, včetně rizik souvisejících s aplikacemi a softwarovými systémy.

11.2 ISO/IEC 27002

11.2.1 Opatření 8.25 – Doporučuje zavést postupy bezpečného návrhu, vývoje a přezkumu kódu pro všechny aplikace, včetně těch dodávaných dodavateli.

11.2.2 Opatření 8.26 – Doporučuje formální testování bezpečnostních opatření aplikací, zejména v oblastech řízení přístupu, ověření vstupů a řízení relací.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Stanoví požadavky na testování vývojáři, analýzu kódu a dynamické skenování aplikací před nasazením.

11.3.2 SI-10 – Zaměřuje se na detekci a prevenci běžných softwarových chyb se zdůrazněním povědomí vývojářů a technických ochranných opatření.

11.4 GDPR EU (2016/679)

11.4.1 Článek 25 – „Ochrana osobních údajů již od návrhu a ve výchozím nastavení“ vyžaduje zabudování ochrany soukromí a zabezpečení do základního návrhu aplikací zpracovávajících osobní údaje.

11.5 směrnice EU NIS2 (2022/2555)

11.5.1 Článek 21 odst. 2 písm. a) a e) – Vyžaduje, aby základní a významné subjekty zavedly technická opatření k zabezpečení aplikací a detekci rizik souvisejících se softwarem.

11.6 nařízení EU DORA (2022/2554)

11.6.1 Článek 9 odst. 2 písm. c), 10 odst. 2 písm. c) – Vyžaduje, aby SME ve finančním sektoru zavedly bezpečnostní opatření na aplikační úrovni a prováděly pravidelná hodnocení k zachování digitální provozní odolnosti.

11.7 COBIT 2019

11.7.1 BAI03 – „Řízení identifikace a tvorby řešení“ poskytuje vodítka pro vývoj nebo pořízení bezpečného softwaru v souladu s riziky, požadavky na soulad a obchodními požadavky, a to i v prostředích SME s omezenými zdroji.