					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P01					Název dokumentu: **Politika informační bezpečnosti**							
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**

1. Účel

1.1 Tato politika stanoví zastřešující závazek organizace k bezpečnosti informací prostřednictvím zavedení formálního systému řízení bezpečnosti informací (ISMS).

1.2 Poskytuje strategické směřování a stanoví základní požadavky na ochranu důvěrnosti, integrity, dostupnosti a odolnosti všech informačních aktiv ve fyzických, digitálních a cloudových prostředích.

1.3 Tato politika naplňuje požadavky ISO/IEC 27001:2022, kapitol 5.1 a 5.2, tím, že vyjadřuje záměr vedení, závazek vrcholového vedení a sladění bezpečnostních činností s cíli organizace.

1.4 Slouží jako závazný referenční dokument pro všechny podřízené politiky, standardy a postupy v rámci ISMS a je nezbytná pro zajištění bezpečnostního prostředí založeného na řízení rizik, souladu a neustálém zlepšování.

2. Rozsah

2.1 Tato politika se vztahuje na všechny osoby, aktiva a procesy vymezené v rozsahu ISMS, včetně:

2.1.1 všech obchodních jednotek, oddělení, dceřiných společností a poboček,

2.1.2 zaměstnanců, smluvních pracovníků, dočasných pracovníků, konzultantů a poskytovatelů služeb třetích stran,

2.1.3 všech dat, informačních systémů, aplikací, infrastruktury a komunikačních kanálů,

2.1.4 všech fyzických, cloudových, vzdálených a hybridních prostředí, v nichž jsou zpracovávána firemní data nebo z nichž je k nim přistupováno.

2.2 Tato politika je závazná pro všechny subjekty nakládající s informacemi organizace a vztahuje se na všechny fáze životního cyklu informací — od vytvoření a přenosu až po ukládání a likvidaci.

2.3 Jakékoli výluky nebo omezení tohoto rozsahu musí být zdokumentovány v Prohlášení o rozsahu ISMS a odůvodněny formálním schválením vrcholovým vedením.

3. Cíle

3.1 Zavést ISMS, který je v souladu s ISO/IEC 27001:2022 a podporuje rozhodování založené na rizicích napříč organizací.

3.2 Zajistit, aby zásady důvěrnosti, integrity a dostupnosti byly začleněny do všech činností organizace, systémů a partnerství.

3.3 Zajistit soulad s právními předpisy a smluvními požadavky prostřednictvím stanovení měřitelných bezpečnostních cílů vycházejících z politik a jejich integrace do provozních činností.

3.4 Minimalizovat pravděpodobnost a dopad incidentů informační bezpečnosti prostřednictvím účinných preventivních, detekčních a nápravných opatření.

3.5 Podporovat neustálé zvyšování vyspělosti informační bezpečnosti prostřednictvím definovaných ukazatelů výkonnosti, výsledků auditů a přezkoumání vedením.

3.6 Rozvíjet kulturu odpovědnosti, povědomí a odolnosti, v níž veškerý personál rozumí svým bezpečnostním odpovědnostem a plní je.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje a potvrzuje Politiku informační bezpečnosti a rámec ISMS.

4.1.2 Zajišťuje soulad mezi bezpečnostními cíli a obchodní strategií.

4.1.3 Jde příkladem a podporuje silnou kulturu bezpečnosti informací.

4.1.4 Přezkoumává a schvaluje zásadní změny rozsahu ISMS, ošetření rizik a struktury správy a řízení.

4.2 Ředitel informační bezpečnosti (CISO) / manažer ISMS

4.2.1 Odpovídá za ISMS a udržuje tuto politiku v souladu s ISO/IEC 27001.

4.2.2 Řídí hodnocení rizik, zavádění opatření a procesy neustálého zlepšování.

4.2.3 Zajišťuje mezioborovou koordinaci bezpečnostních aktivit a vykonává dohled nad podřízenými politikami.

4.2.4 Podává vrcholovému vedení zprávy o stavu ISMS, incidentech, výsledcích auditů a metrikách.

4.2.5 Zajišťuje, aby přezkum a aktualizace politiky probíhaly v souladu s kapitolou 9 tohoto dokumentu.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Frekvence přezkumu

9.1.1 Tato politika musí být přezkoumána nejméně jednou ročně nebo při vzniku některého z následujících podnětů:

9.1.1.1 významné změny právních, regulatorních nebo smluvních povinností,

9.1.1.2 podstatné změny rizikového profilu organizace,

9.1.1.3 výstupy z interních nebo externích auditů,

9.1.1.4 závažné incidenty nebo selhání kontrol.

9.2 Pravomoc a proces přezkumu

9.2.1 Proces přezkumu řídí CISO nebo určený manažer ISMS.

9.2.2 Podklady pro přezkum musí zahrnovat:

9.2.2.1 výsledky interního auditu,

9.2.2.2 trendy v hodnocení rizik,

9.2.2.3 změny obchodních procesů a technologií,

9.2.2.4 plnění KPI a prahových hodnot rizik.

9.2.3 Všechny aktualizace musí:

9.2.3.1 být řízeny v režimu správy verzí a zdokumentovány,

9.2.3.2 být schváleny vrcholovým vedením,

9.2.3.3 být distribuovány všem dotčeným stranám prostřednictvím oficiálních komunikačních kanálů,

9.2.3.4 vyvolat nezbytné aktualizace podřízené dokumentace a školení.

10. Související politiky a vazby

10.1 Tato základní politika je přímo provázána s následujícími organizačními bezpečnostními politikami a rámci:

10.1.1 P2 – Politika rolí a odpovědností ve správě a řízení: vymezuje strukturu správy a řízení a hierarchii pravomocí, na které tento dokument odkazuje.

10.1.2 P3 – Zásady přípustného užívání: stanoví požadavky na chování a přípustné nakládání s informačními aktivy.

10.1.3 P4 – Politika řízení přístupu: operacionalizuje opatření související s přístupem vycházející z této zastřešující politiky.

10.1.4 P6 – Politika řízení rizik: poskytuje kontext založený na rizicích pro výběr opatření a přijímání zbytkových rizik.

10.1.5 P33 – Politika monitorování auditu a souladu: stanoví, jak interní mechanismy zajištění ověřují uplatňování politiky.

10.2 Tyto vzájemné vazby zajišťují komplexní soulad a dohledatelnost napříč ISMS a podporují jednotnou správu a řízení rizik a souladu.

11. Referenční normy a rámce

11.1 Tato Politika informační bezpečnosti je formálně sladěna s následujícími normami a rámci, aby byl zajištěn úplný soulad, připravenost na audit a obhajitelnost vůči regulatorním požadavkům:

11.2 ISO/IEC 27001

11.2.1 Kapitola 5.1 – Vedení a závazek: Tato politika dokládá závazek vrcholového vedení k bezpečnosti informací a vymezuje odpovědnosti a přidělení zdrojů pro ISMS.

11.2.2 Kapitola 5.2 – Politika informační bezpečnosti: Tento dokument slouží jako formální bezpečnostní politika organizace v souladu se stanovenými bezpečnostními cíli, obchodní strategií a požadavky ISO/IEC 27001.

11.2.3 Kapitola 6.1 – Opatření k řešení rizik a příležitostí: Přístup založený na rizicích uplatněný v této politice zajišťuje, že bezpečnostní zdroje jsou používány přiměřeně hrozbám.

11.2.4 Kapitola 9.2 – interní audit a kapitola 10 – zlepšování: Tato politika je začleněna do životního cyklu neustálého zlepšování organizace a podléhá ověřování interním auditem.

11.2.5 ISO/IEC 27002:2022 – Opatření 5.1: Stanoví pokyny pro zavedení a udržování bezpečnostních politik. Tato politika odráží doporučení ISO/IEC 27002 pro hierarchickou dokumentaci, cykly přezkumu a vymahatelnost.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Politika a postupy plánování bezpečnosti): Tato politika naplňuje požadavek na vytvoření, zveřejnění a přezkoumávání formální politiky informační bezpečnosti pro celou organizaci.

11.3.2 PM-1 až PM-5: Pokrývá správu a řízení na úrovni programu včetně rolí v oblasti bezpečnosti informací, přidělování zdrojů, strategie řízení rizik a integrace bezpečnostního plánování do provozu organizace.

11.4 GDPR (2016/679)

11.4.1 Článek 5 odst. 2: Prosazuje zásadu odpovědnosti. Tato politika vymezuje odpovědné osoby a dohledatelné kroky při uplatňování požadavků.

11.4.2 Článek 24: Vyžaduje zavedení technických a organizačních opatření, včetně politik sladěných s riziky.

11.4.3 Článek 32: Podporuje zavedení přiměřených opatření k zajištění zabezpečení osobních údajů po celý jejich životní cyklus.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21 odst. 2 písm. a): Ukládá subjektům povinnost zavést dokumentovanou bezpečnostní politiku řešící řízení rizik a správu a řízení. Tato politika tento požadavek plní a podporuje širší připravenost na kybernetickou bezpečnost a ochranu kritické infrastruktury.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 5 odst. 2: Vyžaduje dokumentovaný rámec vnitřních kontrol pro řízení rizik v oblasti ICT. Tato politika podporuje soulad ve finančním sektoru tím, že přiřazuje role, opatření a dohledové funkce v souladu s očekáváními DORA v oblasti správy a řízení.

11.7 COBIT 2019

11.7.1 EDM01 – Nastavení rámce správy a řízení: Tato politika podporuje správu a řízení podniku tím, že vymezuje role ISMS, závazky vedení a strategické cíle.

11.7.2 APO01 – Rámec řízení: Podporuje zavedení a provoz strukturovaného ISMS.

11.7.3 APO12 – Řízení rizik: Poskytuje základ pro správu a řízení rizik bezpečnosti informací.

11.7.4 MEA01/MEA03 – Monitorování, vyhodnocování a posuzování: Posiluje průběžné vyhodnocování výkonnosti a monitorování vnitřních kontrol prostřednictvím prosazování souladu s politikou.