					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P01					Názov dokumentu: **Politika informačnej bezpečnosti**							
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**

1. Účel

1.1 Táto politika stanovuje zastrešujúci záväzok organizácie k informačnej bezpečnosti prostredníctvom zavedenia formálneho systému manažérstva informačnej bezpečnosti (ISMS).

1.2 Poskytuje strategické smerovanie a základné požiadavky na ochranu dôvernosti, integrity, dostupnosti a odolnosti všetkých informačných aktív vo fyzickom, digitálnom a cloudovom prostredí.

1.3 Táto politika napĺňa požiadavky kapitol 5.1 a 5.2 normy ISO/IEC 27001:2022 tým, že vyjadruje zámer vedenia, záväzok vrcholového manažmentu a zosúladenie bezpečnostných činností s cieľmi organizácie.

1.4 Slúži ako záväzný referenčný dokument pre všetky podriadené politiky, normy a postupy v rámci ISMS a je nevyhnutná na vytvorenie bezpečnostného prostredia založeného na riadení rizík, súlade a neustálom zlepšovaní.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky osoby, aktíva a procesy vymedzené v rozsahu ISMS, vrátane:

2.1.1 všetkých obchodných útvarov, oddelení, dcérskych spoločností a pobočiek,

2.1.2 zamestnancov, zmluvných pracovníkov, dočasných pracovníkov, konzultantov a poskytovateľov služieb tretích strán,

2.1.3 všetkých údajov, informačných systémov, aplikácií, infraštruktúry a komunikačných kanálov,

2.1.4 všetkých fyzických, cloudových, vzdialených a hybridných prostredí, v ktorých sa spracúvajú údaje organizácie alebo sa k nim pristupuje.

2.2 Táto politika je záväzná pre všetky subjekty nakladajúce s informáciami organizácie a vzťahuje sa na všetky fázy životného cyklu informácií — od ich vytvorenia a prenosu až po uchovávanie a likvidáciu.

2.3 Akékoľvek vylúčenia alebo obmedzenia tohto rozsahu musia byť zdokumentované vo vyhlásení o rozsahu ISMS a odôvodnené formálnym schválením výkonného manažmentu.

3. Ciele

3.1 Zaviesť ISMS, ktorý je v súlade s ISO/IEC 27001:2022 a podporuje rozhodovanie založené na rizikách v celej organizácii.

3.2 Zabezpečiť, aby princípy dôvernosti, integrity a dostupnosti boli začlenené do všetkých činností, systémov a partnerstiev organizácie.

3.3 Umožniť plnenie regulačných a zmluvných požiadaviek vymedzením merateľných bezpečnostných cieľov založených na politikách a ich integráciou do prevádzky organizácie.

3.4 Minimalizovať pravdepodobnosť a dopad incidentov informačnej bezpečnosti prostredníctvom účinných preventívnych, detekčných a nápravných kontrol.

3.5 Podporovať neustále zlepšovanie úrovne vyspelosti informačnej bezpečnosti prostredníctvom definovaných ukazovateľov výkonnosti, výsledkov auditov a preskúmania manažmentom.

3.6 Presadzovať kultúru zodpovednosti, povedomia a odolnosti, v ktorej všetci pracovníci rozumejú svojim bezpečnostným povinnostiam a plnia ich.

4. Roly a zodpovednosti

4.1 Výkonný manažment

4.1.1 Schvaľuje a potvrdzuje Politiku informačnej bezpečnosti a rámec ISMS.

4.1.2 Zabezpečuje zosúladenie bezpečnostných cieľov s obchodnou stratégiou.

4.1.3 Ide príkladom a podporuje silnú kultúru informačnej bezpečnosti.

4.1.4 Preskúmava a schvaľuje významné zmeny rozsahu ISMS, spôsobu ošetrenia rizík a riadiacej štruktúry.

4.2 Riaditeľ informačnej bezpečnosti (CISO) / manažér ISMS

4.2.1 Je vlastníkom ISMS a zabezpečuje súlad tejto politiky s ISO/IEC 27001.

4.2.2 Vedie procesy posudzovania rizík, implementácie kontrol a neustáleho zlepšovania.

4.2.3 Zabezpečuje koordináciu bezpečnostných činností naprieč funkciami a vykonáva dohľad nad podriadenými politikami.

4.2.4 Predkladá výkonnému manažmentu správy o stave ISMS, incidentoch, výsledkoch auditov a metrikách.

4.2.5 Zabezpečuje, aby sa preskúmania a aktualizácie politiky vykonávali v súlade s oddielom 9 tohto dokumentu.

[... 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 Frekvencia preskúmania

9.1.1 Táto politika sa musí preskúmavať najmenej raz ročne alebo pri splnení niektorej z týchto podmienok:

9.1.1.1 významné zmeny právnych, regulačných alebo zmluvných povinností,

9.1.1.2 významné zmeny rizikového profilu organizácie,

9.1.1.3 výstupy z interných alebo externých auditov,

9.1.1.4 závažné incidenty alebo zlyhania kontrol.

9.2 Autorita a proces preskúmania

9.2.1 Proces preskúmania vedie CISO alebo určený manažér ISMS.

9.2.2 Vstupy do preskúmania musia zahŕňať:

9.2.2.1 výsledky vnútorného auditu,

9.2.2.2 trendy v posudzovaní rizík,

9.2.2.3 zmeny obchodných procesov a technológií,

9.2.2.4 plnenie KPI a rizikových prahov.

9.2.3 Všetky aktualizácie musia:

9.2.3.1 podliehať verzovaniu a byť zdokumentované,

9.2.3.2 byť schválené výkonným manažmentom,

9.2.3.3 byť distribuované všetkým dotknutým stranám prostredníctvom oficiálnych komunikačných kanálov,

9.2.3.4 vyvolať potrebné aktualizácie podriadenej dokumentácie a školení.

10. Súvisiace politiky a väzby

10.1 Táto základná politika je priamo prepojená s týmito bezpečnostnými politikami a rámcami organizácie:

10.1.1 P2 – Politika rolí a zodpovedností správy a riadenia: vymedzuje štruktúru správy a riadenia a hierarchiu právomocí, na ktoré sa tento dokument odvoláva.

10.1.2 P3 – Politika prijateľného používania: upravuje pravidlá správania a prípustné používanie informačných aktív.

10.1.3 P4 – Politika riadenia prístupu: konkretizuje kontroly súvisiace s prístupom odvodené od tejto zastrešujúcej politiky.

10.1.4 P6 – Politika riadenia rizík: poskytuje kontext založený na rizikách pre výber kontrol a akceptáciu reziduálnych rizík.

10.1.5 P33 – Politika monitorovania, auditu a súladu: podrobne určuje, ako interné mechanizmy uisťovania overujú uplatňovanie politiky.

10.2 Tieto vzájomné väzby zabezpečujú komplexné zosúladenie a sledovateľnosť v rámci ISMS a podporujú jednotnú správu a riadenie rizík a súladu.

11. Referenčné normy a rámce

11.1 Táto Politika informačnej bezpečnosti je formálne zosúladená s týmito normami a rámcami s cieľom zabezpečiť úplný súlad, pripravenosť na audit a obhájiteľnosť voči regulačným požiadavkám:

11.2 ISO/IEC 27001

11.2.1 Kapitola 5.1 – Vedenie a záväzok: Táto politika preukazuje záväzok vrcholového manažmentu k informačnej bezpečnosti a vymedzuje zodpovednosti a prideľovanie zdrojov pre ISMS.

11.2.2 Kapitola 5.2 – Politika informačnej bezpečnosti: Tento dokument slúži ako formálna bezpečnostná politika organizácie, zosúladená so stanovenými bezpečnostnými cieľmi, obchodnou stratégiou a požiadavkami ISO/IEC 27001.

11.2.3 Kapitola 6.1 – Opatrenia na riešenie rizík a príležitostí: Prístup založený na rizikách premietnutý do tejto politiky zabezpečuje, aby sa bezpečnostné zdroje uplatňovali primerane hrozbám.

11.2.4 Kapitola 9.2 – Vnútorný audit a kapitola 10 – Zlepšovanie: Táto politika je začlenená do cyklu neustáleho zlepšovania organizácie a podlieha overeniu vnútorným auditom.

11.2.5 ISO/IEC 27002:2022 – Kontrola 5.1: Poskytuje usmernenia na vytváranie a udržiavanie bezpečnostných politík. Táto politika odráža odporúčania ISO/IEC 27002 pre hierarchickú dokumentáciu, cykly preskúmania a záväznosť.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Politika a postupy bezpečnostného plánovania): Táto politika spĺňa požiadavku na vypracovanie, komunikovanie a preskúmavanie formálnej celoorganizačnej politiky informačnej bezpečnosti.

11.3.2 PM-1 až PM-5: Upravuje správu a riadenie na úrovni programu vrátane rolí informačnej bezpečnosti, prideľovania zdrojov, stratégie riadenia rizík a integrácie bezpečnostného plánovania do podnikovej prevádzky.

11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 5(2): Presadzuje zásadu zodpovednosti. Táto politika určuje zodpovedné strany a sledovateľné opatrenia na uplatňovanie politiky.

11.4.2 Článok 24: Vyžaduje implementáciu technických a organizačných opatrení vrátane politík zosúladených s rizikami.

11.4.3 Článok 32: Podporuje implementáciu primeraných opatrení na zabezpečenie ochrany osobných údajov počas celého ich životného cyklu.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(a): Ukladá subjektom povinnosť implementovať zdokumentovanú bezpečnostnú politiku zameranú na riadenie rizík a správu a riadenie. Táto politika túto požiadavku spĺňa a podporuje širšiu pripravenosť na kybernetickú bezpečnosť a ochranu kritickej infraštruktúry.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 5(2): Vyžaduje zdokumentovaný rámec vnútornej kontroly pre riadenie rizík IKT. Táto politika podporuje súlad finančného sektora tým, že priraďuje roly, kontroly a funkcie dohľadu v súlade s očakávaniami DORA v oblasti správy a riadenia.

11.7 COBIT 2019

11.7.1 EDM01 – Nastavenie rámca správy a riadenia: Táto politika podporuje podnikovú správu a riadenie vymedzením rolí ISMS, záväzkov vedenia a strategických cieľov.

11.7.2 APO01 – Rámec riadenia: Podporuje zavedenie a prevádzku štruktúrovaného ISMS.

11.7.3 APO12 – Riadenie rizík: Poskytuje základ pre správu a riadenie rizík informačnej bezpečnosti.

11.7.4 MEA01/MEA03 – Monitorovanie, hodnotenie a posudzovanie: Posilňuje priebežné hodnotenie výkonnosti a monitorovanie vnútorných kontrol prostredníctvom uplatňovania súladu s politikou.