					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P01S					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**

V souladu s normami a právními předpisy

Norma/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitoly 5.1, 5.2, 5.3, 6.1, 6.2, 8	Stanoví závazek vedení, požadavky na politiku, přiřazení rolí, hodnocení rizik a provozní řízení.
ISO/IEC 27002:2022	Opatření 5.1–5.5	Stanoví požadavky na tvorbu dokumentovaných politik informační bezpečnosti, přiřazení rolí, oddělení povinností a odpovědnosti vedení.
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Stanoví požadavky na plán bezpečnostního programu, politiku plánování, hodnocení a autorizaci a řízení přístupu.
GDPR EU (2016/679)	Článek 5 odst. 2, článek 32	Stanoví zásadu odpovědnosti a opatření k zabezpečení zpracování, zejména s ohledem na dokumentované role.
Směrnice EU NIS2 (2022/2555)	Článek 21 odst. 2 písm. a)	Vyžaduje opatření k řízení rizik a vymezení rolí a odpovědností za kybernetická rizika.
Nařízení EU DORA (2022/2554)	Článek 9, článek 10	Vyžaduje přiřazení rolí pro řízení ICT rizik a zajištění kontinuity činností.
COBIT 2019	EDM03, APO13, DSS05	Podporuje optimalizaci rizik, řízení bezpečnosti a řízení bezpečnostních služeb prostřednictvím jasného přiřazení rolí.

1. Účel

1.1 Tato politika vyjadřuje závazek organizace chránit informace zákazníků a obchodní informace prostřednictvím jasného vymezení odpovědností a praktických bezpečnostních opatření přiměřených organizacím bez vyčleněných IT týmů.

1.2 Zajišťuje, aby všichni zaměstnanci, smluvní pracovníci a poskytovatelé služeb dodržovali závazná pravidla, která umožňují plný soulad s požadavky certifikace ISO/IEC 27001.

1.3 Tato politika umožňuje organizaci budovat důvěru zákazníků tím, že jednoznačně dokládá, jak chrání jejich informace prostřednictvím vymezených odpovědností, strukturovaných procesů a jasně stanovené odpovědnosti.

2. Rozsah

2.1 Tato politika se vztahuje na všechny osoby, které přistupují k datům a systémům organizace nebo je spravují, včetně:

2.1.1 vlastníků společnosti a generálních ředitelů

2.1.2 zaměstnanců, smluvních pracovníků a stážistů

2.1.3 externích poskytovatelů IT služeb nebo konzultantů

2.2 Vztahuje se na všechny typy informací, systémů a služeb, včetně:

2.2.1 obchodních záznamů, zákaznických dat, hesel a e-mailů

2.2.2 IT hardwaru, jako jsou notebooky a telefony

2.2.3 cloudových služeb používaných pro ukládání souborů, komunikaci nebo finance

2.2.4 fyzických dokumentů uložených v kancelářských prostorách

2.3 Tato politika platí ve všech pracovních prostředích – v kanceláři, při práci na dálku i v cloudu – a zahrnuje všechna zařízení a software používané ke zpracování nebo ukládání obchodních informací.

3. Cíle

3.1 Jasně přiřadit odpovědnost: Zajistit, aby za informační bezpečnost vždy odpovídala konkrétní osoba. Obvykle jde o generálního ředitele nebo osobu, kterou formálně pověří.

3.2 Chránit informace zákazníků a obchodní informace: Zavést spolehlivá a konzistentní ochranná opatření, která zabrání zneužití, ztrátě nebo odcizení citlivých údajů, včetně zákaznických a finančních záznamů.

3.3 Podpořit certifikaci ISO/IEC 27001: Umožnit organizaci doložit plný soulad s požadavky ISO/IEC 27001 a zajistit připravenost na audit i způsobilost k certifikaci bez nutnosti složité infrastruktury.

3.4 Začlenit bezpečnost do obchodních činností: Integrovat informační bezpečnost do každodenních činností a rozhodování v celé organizaci.

3.5 Budovat bezpečnostní povědomí a kulturu: Zajistit, aby každý zaměstnanec rozuměl bezpečnostním postupům a dodržoval je, například používáním silných hesel a hlášením podezřelé činnosti.

4. Role a odpovědnosti

4.1 Generální ředitel nebo vlastník společnosti

4.1.1 Nese celkovou odpovědnost za informační bezpečnost.

4.1.2 Schvaluje tuto politiku a odpovídá za její udržování.

4.1.3 Zajišťuje, aby všechny klíčové bezpečnostní činnosti byly buď vykonávány přímo, nebo písemně delegovány.

4.1.4 Ověřuje, že všechny delegované bezpečnostní činnosti (například řízení přístupu nebo reakce na incidenty) jsou vykonávány účinně.

4.1.5 Působí jako primární kontaktní osoba pro všechny interní i externí záležitosti týkající se bezpečnosti, včetně auditů a dotazů zákazníků.

4.1.6 V rámci každoročního přezkumu sleduje plnění těchto cílů. Cíle mají být, kde je to možné, měřitelné (např. % proškolených pracovníků, počet nahlášených incidentů apod.) a musí být aktualizovány podle bezpečnostních zjištění a změn rizik.

4.2 Určený zaměstnanec (je-li relevantní)

4.2.1 Může podporovat generálního ředitele při řízení každodenních činností, jako je zřizování uživatelských účtů, odebírání přístupu odcházejícím pracovníkům nebo koordinace s poskytovatelem IT služeb.

4.2.2 Musí být formálně pověřen a musí mít dostatečnou pravomoc a nástroje k výkonu těchto činností.

4.2.3 Všechny problémy hlásí generálnímu řediteli.

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

9. Požadavky na přezkum a aktualizaci

9.1 Každoroční přezkum

9.1.1 Tuto politiku musí generální ředitel (GM) přezkoumat nejméně jednou ročně, aby byl zajištěn trvalý soulad s požadavky certifikace ISO/IEC 27001, změnami právních předpisů (například GDPR, NIS2 a DORA) a vyvíjejícími se potřebami organizace.

9.2 Mimořádné přezkumy

9.2.1 Další přezkumy musí proběhnout vždy, když nastanou významné změny, například:

9.2.1.1 závažné bezpečnostní incidenty nebo porušení zabezpečení dat

9.2.1.2 zavedení nových obchodních procesů nebo technologií (např. nového softwaru, platforem pro práci na dálku nebo cloudových služeb)

9.2.1.3 změny právních nebo regulačních požadavků ovlivňujících nakládání s informacemi

9.3 Dokumentace změn

9.3.1 Všechny přezkumy a změny této politiky musí být formálně zdokumentovány s jasným uvedením data, povahy úprav a schválení GM.

9.3.2 Historie verzí politiky musí být bezpečně uchovávána, aby bylo možné během auditů doložit vývoj politiky a soulad.

9.4 Komunikace aktualizací

9.4.1 Jakékoli změny této politiky musí být neprodleně oznámeny všem zaměstnancům, smluvním pracovníkům a relevantním třetím stranám.

9.4.2 Aktualizované verze politiky musí být snadno dostupné všem dotčeným osobám (např. elektronickým sdílením nebo fyzickým vyvěšením na pracovišti).

10. Související politiky a návaznosti

10.1 Tato politika úzce souvisí s dalšími politikami v sadě SME politik organizace, konkrétně:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Upřesňuje přiřazení bezpečnostních povinností a odpovědností.

10.1.2 P4S – Politika řízení přístupu: Vymezuje bezpečné nakládání s přístupy k firemním informacím.

10.1.3 P8S – Politika bezpečnostního povědomí a školení: Poskytuje základní pokyny pro školení pracovníků a budování povědomí.

10.1.4 P17S – Politika ochrany osobních údajů a soukromí: Zajišťuje soulad s GDPR a dalšími právními předpisy v oblasti ochrany osobních údajů.

10.1.5 P30S – Politika reakce na incidenty: Popisuje podrobné kroky požadované při reakci na bezpečnostní incidenty.

10.2 Tyto navazující politiky poskytují jasné provozní pokyny a musí být zaváděny společně, aby bylo dosaženo plného souladu s požadavky certifikace ISO/IEC 27001.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 5.1 – Vedení a závazek: Vyžaduje závazek vrcholového vedení a odpovědnost za účinnost informační bezpečnosti v organizaci.

11.1.2 Kapitola 5.2 – Politika informační bezpečnosti: Ukládá jasné, dokumentované politiky sladěné se strategií organizace a požadavky na soulad.

11.1.3 Kapitola 5.3 – Organizační role a odpovědnosti: Vymezuje jasné přiřazení odpovědností za informační bezpečnost v celé organizaci, což je nezbytné pro účinnou správu a řízení i auditní soulad.

11.1.4 Kapitola 6.1 – Opatření k řešení rizik a příležitostí: Zajišťuje, aby rizika informační bezpečnosti byla systematicky identifikována, vyhodnocována a ošetřována.

11.1.5 Kapitola 8.1 – Provozní plánování a řízení: Vyžaduje, aby organizace plánovala a zaváděla procesy potřebné ke splnění cílů informační bezpečnosti a účinnému řízení souvisejících rizik.

11.2 ISO/IEC 27002:2022 Opatření 5.1–5.5

11.2.1 Příloha A, opatření 5.1 – Politiky informační bezpečnosti: Stanoví tvorbu a komunikaci dokumentovaných politik informační bezpečnosti.

11.2.2 Příloha A, opatření 5.2 – Role a odpovědnosti v oblasti informační bezpečnosti: Upřesňuje a formálně přiřazuje role a odpovědnosti v oblasti informační bezpečnosti relevantním stranám.

11.2.3 Příloha A, opatření 5.3 – Oddělení povinností: Vyžaduje jasné oddělení povinností ke snížení střetu zájmů a rizika podvodu při nakládání s citlivými informacemi.

11.2.4 Příloha A, opatření 5.4 – Odpovědnosti vedení: Ukládá vedení, aby prokazovalo závazek k informační bezpečnosti prostřednictvím aktivního dohledu a přidělení zdrojů.

11.2.5 Příloha A, opatření 5.5 – Kontakty s orgány veřejné moci: Posiluje potřebu jasně dokumentovaných politik informační bezpečnosti, rolí, odpovědností a struktur správy a řízení, a tím zajišťuje konzistentní řízení a auditní stopu v celé organizaci.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plán programu informační bezpečnosti: Vyžaduje dokumentované strategie a politiky správy informační bezpečnosti a poskytuje rámec pro konzistentní implementaci a řízení.

11.3.2 PL-1 – Politika plánování bezpečnosti: Ukládá celopodnikovou politiku plánování bezpečnosti, která usměrňuje bezpečný provoz a strategické sladění činností informační bezpečnosti.

11.3.3 CA-1 – Politika hodnocení a autorizace bezpečnosti: Vyžaduje jasně definované role pro hodnocení a autorizaci, aby byla zajištěna průběžná účinnost a soulad s požadavky informační bezpečnosti.

11.3.4 AC-1 – Politika řízení přístupu: Vyžaduje, aby organizace jasně vymezily, dokumentovaly a prosazovaly postupy a odpovědnosti v oblasti řízení přístupu.

11.4 GDPR EU (2016/679)

11.4.1 Článek 5 odst. 2 – Zásada odpovědnosti: Vyžaduje, aby organizace doložily soulad se zásadami ochrany osobních údajů, včetně dokumentovaných rolí a politik pro odpovědnosti v oblasti ochrany osobních údajů.

11.4.2 Článek 32 – Zabezpečení zpracování: Ukládá zavedení vhodných technických a organizačních opatření, včetně jasných bezpečnostních odpovědností, k ochraně osobních údajů před porušením zabezpečení osobních údajů a neoprávněným přístupem.

11.5 Směrnice EU NIS2 (2022/2555)

11.5.1 Článek 21 odst. 2 písm. a) – Opatření k řízení rizik: Vyžaduje jasné uspořádání správy a řízení, včetně definovaných rolí a odpovědností za informační bezpečnost, což je nezbytné pro účinné řízení kybernetických rizik.

11.6 Nařízení EU DORA (2022/2554)

11.6.1 Článek 9 – Řízení ICT rizik: Vyžaduje, aby organizace jasně přiřadily role a odpovědnosti související s řízením ICT rizik, a tím posílily odolnost a připravenost na zajištění kontinuity činností.

11.6.2 Článek 10 – Kontinuita činností ICT: Vyžaduje jasnou odpovědnost a strukturované role pro udržování odolnosti a kontinuity ICT, aby organizace mohly spolehlivě reagovat na narušení.

11.7 COBIT 2019

11.7.1 EDM03 – Zajištění optimalizace rizik: Zdůrazňuje jasně definovanou odpovědnost a role při řízení organizačních rizik a podporuje silnou správu a řízení a účinný dohled nad riziky informační bezpečnosti.

11.7.2 APO13 – Řízení bezpečnosti: Vyžaduje, aby organizace jasně stanovily a komunikovaly odpovědnosti za řízení bezpečnosti a zajistily jejich soulad s obchodními cíli a regulačními požadavky.

11.7.3 DSS05 – Řízení bezpečnostních služeb: Požaduje strukturované role a jasné odpovědnosti při řízení bezpečnostních služeb, což umožňuje konzistentní implementaci a ověřování souladu.