					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P08S					Název dokumentu: **Politika povědomí o informační bezpečnosti a školení**						
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 7	
ISO/IEC 27002:2022	Opatření 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
směrnice NIS2	Článek 21 odst. 2 písm. i)	
nařízení DORA	Článek 13	
COBIT 2019	BAI08, DSS05	
GDPR	Článek 32, 39	

1. Účel

1.1. Tato politika zajišťuje, aby všichni zaměstnanci a smluvní pracovníci rozuměli svým odpovědnostem v oblasti informační bezpečnosti.

1.2. Jejím cílem je snížit pravděpodobnost lidské chyby, posílit schopnost odhalovat a hlásit incidenty a podporovat kulturu bezpečnostního povědomí v celé organizaci.

1.3. Tato politika podporuje soulad s ISO/IEC 27001, NIS2, GDPR a DORA tím, že začleňuje bezpečnostní povědomí do každodenního pracovního jednání a očekávání podle jednotlivých rolí.

2. Rozsah

2.1. Tato politika se vztahuje na všechny zaměstnance, smluvní pracovníky, stážisty a třetí strany, které mají přístup k firemním systémům nebo datům.

2.2. Zahrnuje:

2.2.1. vstupní školení bezpečnostního povědomí pro nově nastupující pracovníky,

2.2.2. každoroční opakovací školení v oblasti bezpečnosti,

2.2.3. ad hoc aktivity na podporu povědomí (např. sdělení v návaznosti na incidenty, plakáty nebo doporučení).

2.3. Platí pro všechny pracovní role, útvary a místa výkonu práce.

3. Cíle

3.1. Zajistit, aby všichni pracovníci absolvovali včasné, srozumitelné a relevantní školení bezpečnostního povědomí.

3.2. Zajistit, aby zaměstnanci dokázali rozpoznat běžné hrozby, jako jsou phishing, malware a úniky dat, a předcházet jim.

3.3. Zavést evidenci absolvovaných školení za účelem doložení souladu s právními, smluvními a auditními požadavky.

3.4. Udržovat obsah školení aktuální tak, aby odrážel politiky organizace, hrozby a příslušné právní požadavky.

3.5. Podporovat u pracovníků proaktivní přístup, v němž je bezpečnost vnímána jako součást každodenní odpovědnosti.

4. Role a odpovědnosti

4.1. generální ředitel

4.1.1. Schvaluje požadavky na školení a zajišťuje přidělení zdrojů.

4.1.2. Přezkoumává zprávy o absolvování školení a v případě potřeby eskaluje případy nesouladu.

4.2. vedoucí kanceláře / HR

4.2.1. Koordinuje realizaci školení pro nově nastupující pracovníky a každoroční opakovací školení.

4.2.2. Vede záznamy o školeních a evidenci absolvování.

4.2.3. Zajišťuje potvrzení seznámení pracovníků se základními politikami informační bezpečnosti a dohodami o mlčenlivosti.

[... 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. Tato politika musí být každoročně přezkoumána generálním ředitelem a HR tak, aby odrážela aktuální rizika, právní požadavky a potřeby pracovní síly.

9.2. Průběžné aktualizace

9.2.1. Politika a obsah školení musí být rovněž přezkoumány a aktualizovány po:

9.2.1.1. významném bezpečnostním incidentu,

9.2.1.2. právních nebo smluvních změnách,

9.2.1.3. organizační restrukturalizaci nebo migraci systémů.

9.3. Řízení verzí a distribuce

9.3.1. Každá aktualizace musí zahrnovat:

9.3.1.1. číslo verze a datum účinnosti,

9.3.1.2. shrnutí změn,

9.3.1.3. schválení generálním ředitelem,

9.3.1.4. archiv všech předchozích verzí uchovávaný nejméně po dobu tří let.

9.4. Komunikace se zaměstnanci

9.4.1. Aktualizace politiky musí být sděleny všem pracovníkům a v případě podstatných změn musí být získáno potvrzení seznámení.

10. Související politiky a vazby

10.1. Tato politika podporuje následující dokumenty:

10.1.1. P2S – Politika rolí a odpovědností v oblasti správy a řízení: přiřazuje odpovědnost za koordinaci školení a dohled,

10.1.2. P3S – Zásady přípustného užívání: posilují očekávání ohledně chování řešeného ve školení,

10.1.3. P4S – Politika řízení přístupu: zajišťuje, aby uživatelé rozuměli významu zabezpečení přístupu,

10.1.4. P7S – Politika nástupu a ukončení: začleňuje školení do procesu nástupu,

10.1.5. P30S – Politika reakce na incidenty: zajišťuje, aby pracovníci věděli, jak incidenty hlásit včas a správně.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 7.3 – Vyžaduje, aby organizace zajistila, že si pracovníci jsou vědomi svých odpovědností a dopadů na bezpečnost.

11.2. ISO/IEC 27002

11.2.1. Opatření 6.3 – Stanoví očekávání pro rozsah a realizaci bezpečnostního školení.

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Vyžaduje školení bezpečnostního povědomí pro uživatele s přístupem k systémům.

11.3.2. AT-4 – Pokrývá školení podle rolí a důsledky nesouladu.

11.4. GDPR

11.4.1. Článek 32 – Ukládá bezpečnostní opatření včetně školení pracovníků k ochraně osobních údajů.

11.4.2. Článek 39 – Vyžaduje, aby pověřenec pro ochranu osobních údajů tam, kde je to relevantní, vykonával dohled nad povědomím a školením.

11.5. směrnice NIS2

11.5.1. Článek 21 odst. 2 písm. i) – Vyžaduje průběžné programy povědomí o kybernetické bezpečnosti a školení.

11.6. nařízení DORA

11.6.1. Článek 13 – Vyžaduje, aby finanční subjekty zavedly vzdělávání a školení pro všechny pracovníky s odpovědnostmi souvisejícími s ICT.

11.7. COBIT 2019

11.7.1. BAI08 – Řízení znalostí: zajišťuje, aby pracovníci byli způsobilí a proškolení.

11.7.2. DSS05 – Řízení bezpečnostních služeb: zdůrazňuje povědomí jako klíčové ochranné opatření.