					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P08S					Názov dokumentu: **Politika povedomia a školení v oblasti 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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 7	
ISO/IEC 27002:2022	Kontrola 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
Smernica EÚ NIS2	Článok 21(2)(i)	
Nariadenie EÚ DORA	Článok 13	
COBIT 2019	BAI08, DSS	
Nariadenie EÚ GDPR	Článok 32, 39	

1. Účel

1.1. Táto politika zabezpečuje, aby všetci zamestnanci a zmluvní pracovníci rozumeli svojim zodpovednostiam v oblasti informačnej bezpečnosti.

1.2. Jej cieľom je znížiť pravdepodobnosť ľudskej chyby, zlepšiť schopnosť rozpoznať a nahlasovať incidenty a podporovať kultúru bezpečnostného povedomia v celej organizácii.

1.3. Táto politika podporuje súlad s ISO/IEC 27001, NIS2, GDPR a DORA tým, že začleňuje bezpečnostné povedomie do každodenného pracovného správania a očakávaní podľa jednotlivých rolí.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetkých zamestnancov, zmluvných pracovníkov, stážistov a tretie strany, ktoré majú prístup k systémom alebo údajom spoločnosti.

2.2. Zahŕňa:

2.2.1. vstupné školenie v oblasti bezpečnostného povedomia pre nový personál,

2.2.2. pravidelné opakovacie školenie v oblasti bezpečnostného povedomia raz ročne,

2.2.3. ad hoc aktivity na zvyšovanie povedomia (napr. oznámenia súvisiace s incidentmi, plagáty alebo odporúčania).

2.3. Uplatňuje sa na všetky pracovné roly, oddelenia a pracoviská.

3. Ciele

3.1. Zabezpečiť, aby všetci pracovníci absolvovali včasné, zrozumiteľné a relevantné školenie v oblasti bezpečnostného povedomia.

3.2. Poskytnúť zamestnancom schopnosť rozpoznať a vyhnúť sa bežným hrozbám, ako sú phishing, malvér a úniky údajov.

3.3. Zaviesť dokumentovanie absolvovania školení na preukázanie súladu s právnymi, zmluvnými a auditnými požiadavkami.

3.4. Udržiavať aktuálny obsah školení, ktorý odráža politiky organizácie, hrozby a uplatniteľné predpisy.

3.5. Podporovať proaktívny prístup pracovníkov, v rámci ktorého sa bezpečnosť vníma ako súčasť každodennej zodpovednosti.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM)

4.1.1. Schvaľuje požiadavky na školenia a zabezpečuje pridelenie zdrojov.

4.1.2. Preskúmava správy o absolvovaní školení a v prípade potreby eskaluje nesúlad.

4.2. Office Manager / HR

4.2.1. Koordinuje realizáciu školení pre nových zamestnancov a ročných opakovacích školení.

4.2.2. Vedie záznamy o školeniach a záznamy o absolvovaní.

4.2.3. Zabezpečuje potvrdenie oboznámenia sa pracovníkov s kľúčovými bezpečnostnými politikami a dohodami o mlčanlivosti.

[... 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. Ročné preskúmanie

9.1.1. Túto politiku musia Generálny manažér (GM) a HR každoročne preskúmať, aby sa zabezpečilo, že odráža aktuálne riziká, predpisy a potreby pracovnej sily.

9.2. Priebežné aktualizácie

9.2.1. Politika a obsah školení musia byť preskúmané a revidované aj po:

9.2.1.1. významnom bezpečnostnom incidente,

9.2.1.2. právnych alebo zmluvných zmenách,

9.2.1.3. reštrukturalizácii organizácie alebo migrácii systémov.

9.3. Riadenie verzií a distribúcia

9.3.1. Každá aktualizácia musí obsahovať:

9.3.1.1. číslo verzie a dátum účinnosti,

9.3.1.2. súhrn zmien,

9.3.1.3. schválenie Generálnym manažérom (GM),

9.3.1.4. archív všetkých predchádzajúcich verzií uchovávaný najmenej tri roky.

9.4. Komunikácia so zamestnancami

9.4.1. Aktualizácie politiky musia byť oznámené všetkým pracovníkom a pri významných zmenách sa musí získať potvrdenie oboznámenia sa.

10. Súvisiace politiky a väzby

10.1. Táto politika podporuje najmä:

10.1.1. P2S – Politika rolí a zodpovedností správy a riadenia: určuje zodpovednosť za koordináciu školení a dohľad,

10.1.2. P3S – Politika prijateľného používania: posilňuje očakávania týkajúce sa správania riešeného v školeniach,

10.1.3. P4S – Politika riadenia prístupu: zabezpečuje, aby používatelia rozumeli významu bezpečnosti prístupu,

10.1.4. P7S – Politika nástupu a ukončenia: začleňuje školenie do procesu nástupu,

10.1.5. P30S – Politika reakcie na incidenty: zabezpečuje, aby pracovníci vedeli incidenty nahlasovať včas a správne.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 7.3 – vyžaduje, aby organizácie zabezpečili, že pracovníci sú oboznámení so svojimi zodpovednosťami a bezpečnostnými dôsledkami svojej činnosti.

11.2. ISO/IEC 27002

11.2.1. Kontrola 6.3 – stanovuje očakávania pre rozsah a realizáciu bezpečnostných školení.

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – vyžaduje školenie povedomia pre používateľov s prístupom do systémov.

11.3.2. AT-4 – pokrýva školenie podľa rolí a dôsledky nesúladu.

11.4. Nariadenie EÚ GDPR

11.4.1. Článok 32 – vyžaduje bezpečnostné opatrenia vrátane školenia pracovníkov na ochranu osobných údajov.

11.4.2. Článok 39 – vyžaduje, aby zodpovedné osoby dohliadali na povedomie a školenia tam, kde je to uplatniteľné.

11.5. Smernica EÚ NIS2

11.5.1. Článok 21(2)(i) – vyžaduje priebežné programy zvyšovania povedomia a školení v oblasti kybernetickej bezpečnosti.

11.6. Nariadenie EÚ DORA

11.6.1. Článok 13 – vyžaduje, aby finančné subjekty zaviedli vzdelávanie a školenia pre všetkých pracovníkov so zodpovednosťami súvisiacimi s IKT.

11.7. COBIT 2019

11.7.1. BAI08 – Riadenie znalostí: zabezpečuje, aby pracovníci mali potrebnú spôsobilosť a boli vyškolení.

11.7.2. DSS05 – Riadenie bezpečnostných služieb: zdôrazňuje povedomie ako kľúčové ochranné opatrenie.