					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P08					Názov dokumentu: **Politika povedomia a školenia 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 7.3, Príloha A Kontrola 6.3	Stanovuje požiadavky na povedomie a školenia, ktoré táto politika upravuje
ISO/IEC 27002:2022	Kontrola 6	Podporuje primerané školenie povedomia podľa pracovných rolí
NIST SP 800-53 Rev.5	AT-1 až AT-5	Je v súlade s politikou a postupmi, školením povedomia, školením podľa rolí, záznamami o školeniach a kontaktom so skupinami bezpečnosti
GDPR EÚ	Články 32, 39; odôvodnenie 78	Vyžaduje školenie pre osoby spracúvajúce osobné údaje a všeobecné povedomie zamestnancov
Smernica EÚ NIS2	Články 21(2)(a, b), 21(3)	Vyžaduje politiky školení v oblasti rizík a bezpečnosti a iniciatívy na zvyšovanie povedomia
Nariadenie EÚ DORA	Články 5, 8, 13	Vyžaduje povedomie o rizikách IKT a školenia ako súčasť kontrol odolnosti
COBIT 2019	APO07, DSS05, MEA	Posilňuje povedomie pracovnej sily, vzdelávanie používateľov a monitorovanie súladu

1. Účel

1.1 Táto politika stanovuje formálny rámec na zabezpečenie toho, aby si všetci pracovníci boli vedomí svojich povinností v oblasti informačnej bezpečnosti a absolvovali školenia potrebné na ochranu dôvernosti, integrity a dostupnosti informačných aktív.

1.2 Podporuje ISO/IEC 27001, kapitolu 7.3 a Prílohu A, Kontrolu 6.3 tým, že vyžaduje štruktúrovaný program zvyšovania povedomia a školení založený na rizikách, prispôsobený organizačným rolám a vyvíjajúcim sa hrozbám.

1.3 Táto politika prispieva k znižovaniu zraniteľností súvisiacich s ľudským faktorom, podpore bezpečnostne uvedomelého správania a priebežnému upevňovaniu bezpečných postupov v súlade s regulačnými a zmluvnými požiadavkami.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky interné aj externé osoby s prístupom k informačným systémom, údajom alebo priestorom organizácie, vrátane:

2.1.1 zamestnancov (na plný úväzok, čiastočný úväzok, dočasní pracovníci)

2.1.2 zmluvných dodávateľov, konzultantov, dodávateľov a stážistov

2.1.3 tretích strán s logickým alebo fyzickým prístupom na základe servisných dohôd

2.2 Rozsah zahŕňa:

2.2.1 vstupné školenie bezpečnostného povedomia

2.2.2 školenie špecifické pre rolu (napr. vývojári, finančný personál, privilegovaní používatelia)

2.2.3 pravidelné opakovacie školenia a kampane na zvyšovanie povedomia

2.2.4 ad hoc školenia v reakcii na incidenty alebo nové hrozby

2.3 Metódy poskytovania školení podľa tejto politiky zahŕňajú e-learning, prezenčné školenia, simulácie, vedomostné testy, plagáty, bezpečnostné bulletiny a povinné potvrdenia oboznámenia sa.

3. Ciele

3.1 Zabezpečiť, aby všetci pracovníci rozumeli svojim povinnostiam pri ochrane aktív organizácie a pri dodržiavaní bezpečnostných politík.

3.2 Poskytovať priebežné a merateľné školenie povedomia zosúladené s expozíciou riziku podľa rolí.

3.3 Zaviesť bezpečné správanie do každodennej prevádzky posilňovaním postupov, ako je bezpečné používanie hesiel, nahlasovanie incidentov a odolnosť voči phishingu.

3.4 Zabezpečiť dodržiavanie predpisov a pripravenosť na audit v oblasti povinných požiadaviek na školenia informačnej bezpečnosti naprieč odvetviami a jurisdikciami.

3.5 Znižovať bezpečnostné incidenty spôsobené nedbanlivosťou, nevedomosťou alebo nesprávnym úsudkom prostredníctvom formovania správnych návykov a priebežného upevňovania požadovaného správania.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje stratégiu školení v oblasti informačnej bezpečnosti organizácie a zabezpečuje primerané zdroje na jej realizáciu a jej začlenenie medzi podnikové priority.

4.1.2 Monitoruje súlad na úrovni manažmentu a zabezpečuje dodržiavanie tejto politiky vo všetkých oddeleniach.

4.2 CISO / manažér ISMS

4.2.1 Je vlastníkom tejto politiky a definuje rámec povedomia a školení v súlade s rizikami, požiadavkami na súlad a potrebami organizácie.

4.2.2 Dohliada na návrh, poskytovanie, sledovanie a preskúmanie všetkých iniciatív v oblasti bezpečnostných školení.

4.2.3 Zabezpečuje pravidelnú aktualizáciu školení tak, aby zohľadňovali vyvíjajúce sa hrozby a nové technológie.

[... 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 a súvisiaci školiaci program musia byť preskúmavané:

9.1.1.1 každoročne, alebo

9.1.1.2 po závažných incidentoch súvisiacich s ľudskou chybou alebo vnútornou hrozbou

9.1.1.3 pri zavedení významných nových technológií alebo hrozieb

9.1.1.4 v reakcii na zmeny zákonných, zmluvných alebo certifikačných povinností

9.2 Proces preskúmania

9.2.1 Preskúmanie vedie CISO v koordinácii s:

9.2.1.1 oddelením ľudských zdrojov a útvarmi vzdelávania

9.2.1.2 právnym oddelením a zodpovednými osobami pre ochranu osobných údajov

9.2.1.3 funkciami IT bezpečnosti a riadenia operačného rizika

9.2.2 Všetky aktualizácie musia byť:

9.2.2.1 schválené Riadiacim výborom ISMS

9.2.2.2 predmetom riadenia verzií a zdokumentované v registri dokumentácie ISMS

9.2.2.3 komunikované používateľom, ak podstatné zmeny ovplyvnia rozsah školení alebo zodpovednosti

9.3 Správa a riadenie aktualizácie obsahu

9.3.1 Školiace moduly a materiály na zvyšovanie povedomia musia byť preskúmavané každých 12 mesiacov s cieľom zabezpečiť:

9.3.1.1 relevantnosť vzhľadom na prostredie hrozieb

9.3.1.2 správnosť z pohľadu regulačných požiadaviek

9.3.1.3 kompatibilitu formátu (napr. prístupnosť, lokalizácia)

9.3.2 Zastaraný alebo zavádzajúci obsah musí byť bezodkladne stiahnutý a nahradený schválenými alternatívami.

10. Súvisiace politiky a väzby

10.1 Túto politiku podporujú a jej uplatňovanie ďalej podporujú tieto dokumenty:

10.1.1 P01 – Politika informačnej bezpečnosti: stanovuje bezpečnostné povedomie ako základné opatrenie v systéme manažérstva informačnej bezpečnosti organizácie.

10.1.2 P03 – Politika prijateľného používania: vyžaduje potvrdenie oboznámenia sa zo strany používateľa počas školenia a objasňuje zodpovednosti súvisiace s každodenným používaním technológií.

10.1.3 P07 – Politika nástupu a ukončenia pracovného pomeru: zabezpečuje začlenenie školení pri nástupe a ich sledovanie počas celého trvania pracovného vzťahu.

10.1.4 P06 – Politika riadenia rizík: prepája školenia zamerané na ľudský faktor s modelovaním hrozieb a stratégiami znižovania reziduálneho rizika.

10.1.5 P33 – Politika monitorovania, auditu a súladu: potvrdzuje, že opatrenia na zvyšovanie povedomia sú počas auditov prevádzkovo zavedené, merateľné a účinné.

10.2 Tieto politiky spolu tvoria komplexný rámec behaviorálnych kontrol, ktorý integruje povedomie, zodpovednosť za konanie a upevňovanie bezpečnostnej kultúry.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 7.3 – Povedomie: vyžaduje, aby organizácie zabezpečili, že pracovníci sú si vedomí politík informačnej bezpečnosti a svojich povinností. Táto politika uplatňuje túto požiadavku prostredníctvom štruktúrovaného procesu nástupu, pravidelných školení a merateľnej účasti na kampaniach.

11.1.2 Príloha A Kontrola 6.3 – Povedomie, vzdelávanie a školenie v oblasti informačnej bezpečnosti: plne pokryté prostredníctvom vstupných, rolovo orientovaných a priebežných školiacich programov prispôsobených rizikovým profilom používateľov.

11.2 ISO/IEC 27002:2022 – Kontrola 6

11.2.1 Podporuje tvorbu a poskytovanie školení povedomia primeraných pracovným rolám s dôrazom na upevňovanie bezpečného správania a pravidelné aktualizácie na základe spravodajstva o hrozbách a spätnej väzby z auditov.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 až AT-5 (rodina požiadaviek Awareness and Training): Táto politika je v súlade s AT-1 (Policy and Procedures), AT-2 (Awareness Training), AT-3 (Role-Based Training), AT-4 (Security Training Records) a AT-5 (Contact with Security Groups).

11.3.2 IA-5, AC-2: Posilňuje zodpovednosť používateľov za bezpečnú autentifikáciu a prijateľné používanie, čo sú základné výsledky programov zvyšovania povedomia.

11.3.3 IR-1 až IR-8: Pripravenosť na reakciu na incidenty sa posilňuje prostredníctvom cielených kampaní zvyšovania povedomia a simulácií.

11.4 GDPR EÚ (2016/679)

11.4.1 Článok 32 – Bezpečnosť spracúvania: vyžaduje, aby pracovníci nakladajúci s osobnými údajmi boli vyškolení na rozpoznávanie, predchádzanie a nahlasovanie rizík týkajúcich sa osobných údajov. Táto politika zabezpečuje primerané školenie osôb spracúvajúcich osobné údaje a všetkých relevantných rolí.

11.4.2 Článok 39 – Úlohy zodpovednej osoby pre ochranu údajov: zahŕňa zvyšovanie povedomia a školenie pracovníkov zapojených do spracovateľských operácií.

11.4.3 Odôvodnenie 78: podporuje primerané opatrenia na zvyšovanie povedomia s cieľom zabezpečiť robustné bezpečnostné postupy a dodržiavanie politík.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(a, b): vyžaduje, aby subjekty prijali politiky v oblasti analýzy rizík a bezpečnostných školení pre všetkých relevantných pracovníkov. Táto politika túto požiadavku plní zavedením priebežných procesov školení citlivých na rolu.

11.5.2 Článok 21(3): podporuje zvyšovanie povedomia o rizikách kybernetickej bezpečnosti medzi manažmentom a zamestnancami prostredníctvom iniciatív na zvyšovanie povedomia a simulácií.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 13 – Stratégia digitálnej prevádzkovej odolnosti: vyžaduje, aby povedomie o rizikách IKT a školenia boli súčasťou modelu správy a riadenia. Táto politika zabezpečuje riešenie ľudského rizika prostredníctvom priebežného vzdelávania a simulácií hrozieb.

11.6.2 Články 5 a 8: zdôrazňujú význam rámcov vnútorných kontrol, ktorých základnými súčasťami pre odolnosť IKT a kybernetickú hygienu sú povedomie a školenia.

11.7 COBIT 2019

11.7.1 APO07 – Managed Human Resources: posilňuje potrebu rozvíjať povedomie o bezpečnostných povinnostiach a začleniť ho do riadenia pracovnej sily.

11.7.2 DSS05 – Managed Security Services: stanovuje kontroly nad vzdelávaním používateľov a nahlasovaním incidentov, ktoré sú neoddeliteľnou súčasťou tejto politiky.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: vyžaduje preskúmanie účinnosti správania používateľov a dodržiavania politiky; v tejto politike sa to uplatňuje prostredníctvom phishingových testov, vedomostných testov a metrík kampaní zvyšovania povedomia.