					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P08					Název dokumentu: **Politika povědomí o bezpečnosti informací 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**

Právní upozornění (autorská práva a omezení užití)

(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševním vlastnictvím společnosti Clarysec LLC. Žádná jeho část nesmí být kopírována, znovu použita, distribuována ani upravována pro komerční nebo implementační účely bez výslovného písemného souhlasu.

Neoprávněné použití je přísně zakázáno a může vést k právním krokům.

V případě licencování kontaktujte: info@clarysec.com

Soulad se standardy a právními předpisy

Standard/právní předpis	Ustanovení/článek	Komentář
ISO/IEC 27001:2022	Kapitola 7.3, Příloha A, opatření 6.3	Stanoví požadavky na povědomí a školení, které tato politika upravuje
ISO/IEC 27002:2022	Opatření 6	Podporuje odpovídající školení a zvyšování povědomí podle pracovních rolí
NIST SP 800-53 Rev.5	AT-1 až AT-5	Je v souladu s politikami a postupy, školením v oblasti bezpečnostního povědomí, školením podle rolí, záznamy o školení a kontaktem s bezpečnostními skupinami
GDPR	Články 32, 39; bod odůvodnění 78	Vyžaduje školení pro osoby zpracovávající osobní údaje a obecné povědomí zaměstnanců
směrnice NIS2	Články 21(2)(a, b), 21(3)	Vyžaduje politiky školení v oblasti rizik a bezpečnosti a iniciativy na podporu povědomí
nařízení DORA	Články 5, 8, 13	Vyžaduje povědomí o rizicích ICT a školení jako součást kontrol odolnosti
COBIT 2019	APO07, DSS05, MEA	Posiluje povědomí zaměstnanců, vzdělávání uživatelů a monitorování souladu

1. Účel

1.1 Tato politika stanoví formální rámec k zajištění toho, aby si veškerý personál byl vědom svých odpovědností v oblasti bezpečnosti informací a absolvoval školení nezbytné k ochraně důvěrnosti, integrity a dostupnosti informačních aktiv.

1.2 Podporuje kapitolu 7.3 normy ISO/IEC 27001 a Přílohu A, opatření 6.3 tím, že vyžaduje strukturovaný program povědomí a školení založený na rizicích, přizpůsobený organizačním rolím a vyvíjejícím se hrozbám.

1.3 Tato politika přispívá ke snižování zranitelností souvisejících s lidským faktorem, podpoře bezpečnostně uvědomělého chování a průběžnému upevňování bezpečných postupů v souladu s regulačními a smluvními požadavky.

2. Rozsah

2.1 Tato politika se vztahuje na všechny interní i externí osoby s přístupem k informačním systémům, datům nebo prostorám organizace, včetně:

2.1.1 zaměstnanců (na plný úvazek, částečný úvazek, dočasných)

2.1.2 dodavatelů a poskytovatelů služeb třetích stran, konzultantů, smluvních pracovníků a stážistů

2.1.3 třetích stran s logickým nebo fyzickým přístupem na základě smluv o poskytování služeb

2.2 Rozsah zahrnuje:

2.2.1 vstupní školení bezpečnostního povědomí

2.2.2 školení specifická pro role (např. vývojáři, finance, privilegovaní uživatelé)

2.2.3 pravidelná opakovací školení a kampaně na podporu povědomí

2.2.4 ad hoc školení v reakci na incidenty nebo nové hrozby

2.3 Metody realizace školení podle této politiky zahrnují e-learning, prezenční školení, simulace, testy znalostí, plakáty, bezpečnostní zpravodaje a povinná potvrzení seznámení.

3. Cíle

3.1 Zajistit, aby veškerý personál rozuměl svým odpovědnostem při ochraně aktiv organizace a při dodržování bezpečnostních politik.

3.2 Poskytovat průběžné a měřitelné školení v oblasti bezpečnostního povědomí v souladu s mírou rizikové expozice podle jednotlivých rolí.

3.3 Začlenit bezpečné chování do každodenního provozu posilováním postupů, jako je bezpečné používání hesel, hlášení incidentů a odolnost vůči phishingu.

3.4 Zajistit soulad s právními předpisy a připravenost na audit v oblasti požadavků na školení bezpečnosti informací napříč odvětvími a jurisdikcemi.

3.5 Snižovat počet bezpečnostních incidentů způsobených nedbalostí, neznalostí nebo chybným úsudkem prostřednictvím utváření žádoucího chování a průběžného upevňování správných postupů.

4. Role a odpovědnosti

4.1 vrcholové vedení

4.1.1 Schvaluje strategii organizace v oblasti školení bezpečnosti informací a zajišťuje, že jsou pro ni vyčleněny potřebné zdroje a že je začleněna do firemních priorit.

4.1.2 Monitoruje soulad na úrovni vedení a zajišťuje dodržování této politiky napříč odděleními.

4.2 ředitel informační bezpečnosti (CISO) / manažer ISMS

4.2.1 Odpovídá za tuto politiku a vymezuje rámec povědomí a školení v souladu s riziky, požadavky na soulad a potřebami organizace.

4.2.2 Dohlíží na návrh, realizaci, sledování a přezkum všech iniciativ v oblasti bezpečnostního školení.

4.2.3 Zajišťuje, aby byla školení pravidelně aktualizována a odrážela vyvíjející se hrozby a nové technologie.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 četnost přezkumu

9.1.1 Tato politika a související program školení musí být přezkoumány:

9.1.1.1 každoročně, nebo

9.1.1.2 po závažných incidentech zahrnujících lidskou chybu nebo vnitřní hrozbu

9.1.1.3 při zavádění významných nových technologií nebo při vzniku významných nových hrozeb

9.1.1.4 v reakci na změny právních, smluvních nebo certifikačních povinností

9.2 proces přezkumu

9.2.1 Přezkum řídí CISO v koordinaci s:

9.2.1.1 odděleními HR a školení

9.2.1.2 právním oddělením a pověřenci pro ochranu osobních údajů

9.2.1.3 funkcemi IT bezpečnosti a operačního rizika

9.2.2 Všechny aktualizace musí být:

9.2.2.1 schváleny řídicím výborem pro bezpečnost informací

9.2.2.2 vedeny v režimu správy verzí a zdokumentovány v registru dokumentů ISMS

9.2.2.3 sděleny uživatelům, pokud podstatné změny ovlivní rozsah školení nebo odpovědnosti

9.3 správa aktualizací obsahu

9.3.1 Moduly školení a materiály pro podporu povědomí musí být přezkoumávány každých 12 měsíců, aby bylo zajištěno:

9.3.1.1 že odpovídají prostředí hrozeb

9.3.1.2 regulatorní správnost

9.3.1.3 kompatibilita formátu (např. přístupnost, lokalizace)

9.3.2 Zastaralý nebo zavádějící obsah musí být neprodleně stažen a nahrazen schválenými alternativami.

10. Související politiky a vazby

10.1 Tato politika je podporována následujícími politikami a současně podporuje jejich uplatňování:

10.1.1 P01 – Politika informační bezpečnosti: stanoví bezpečnostní povědomí jako základní opatření v rámci ISMS organizace.

10.1.2 P03 – Zásady přípustného užívání: vyžadují potvrzení seznámení uživatele v průběhu školení a vyjasňují odpovědnosti související s každodenním používáním technologií.

10.1.3 P07 – Politika nástupu a ukončení: zajišťuje, aby bylo školení začleněno při nástupu a sledováno po celou dobu pracovního poměru.

10.1.4 P06 – Politika řízení rizik: propojuje školení zaměřené na lidský faktor s modelováním hrozeb a strategiemi snižování zbytkového rizika.

10.1.5 P33 – Politika monitorování auditu a souladu: potvrzuje, že opatření v oblasti povědomí jsou během auditů funkční, měřitelná a účinná.

10.2 Tyto politiky společně tvoří komplexní rámec behaviorálních kontrol, který integruje povědomí, odpovědnost a posilování kultury.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 7.3 – Povědomí: vyžaduje, aby organizace zajistily, že pracovníci znají politiky bezpečnosti informací a své odpovědnosti. Tato politika tento požadavek převádí do praxe prostřednictvím strukturovaného procesu nástupu, pravidelného školení a měřitelné účasti v kampaních.

11.1.2 Příloha A, opatření 6.3 – Povědomí, vzdělávání a školení v oblasti bezpečnosti informací: plně pokryto prostřednictvím vstupních, rolově specifických a průběžných programů školení přizpůsobených rizikovým profilům uživatelů.

11.2 ISO/IEC 27002:2022 – Opatření 6

11.2.1 Podporuje vývoj a realizaci školení v oblasti bezpečnostního povědomí odpovídajícího pracovním rolím se zaměřením na upevňování bezpečného chování a pravidelné aktualizace na základě zpravodajství o hrozbách a zpětné vazby z auditů.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 až AT-5 (oblast Povědomí a školení): Tato politika je v souladu s AT-1 (politika a postupy), AT-2 (školení v oblasti bezpečnostního povědomí), AT-3 (školení podle rolí), AT-4 (záznamy o bezpečnostním školení) a AT-5 (kontakt s bezpečnostními skupinami).

11.3.2 IA-5, AC-2: Posiluje odpovědnost uživatelů za bezpečnou autentizaci a přípustné užívání, což je klíčové pro behaviorální výsledky programů povědomí.

11.3.3 IR-1 až IR-8: Připravenost na reakci na incidenty je posilována prostřednictvím cílených kampaní na podporu povědomí a simulací.

11.4 GDPR (2016/679)

11.4.1 Článek 32 – Zabezpečení zpracování: vyžaduje, aby personál nakládající s osobními údaji byl vyškolen k rozpoznávání, prevenci a hlášení rizik pro osobní údaje. Tato politika zajišťuje odpovídající školení osob zpracovávajících osobní údaje a všech dalších relevantních rolí.

11.4.2 Článek 39 – Úkoly pověřence pro ochranu osobních údajů: zahrnuje zvyšování povědomí a školení pracovníků zapojených do operací zpracování.

11.4.3 Bod odůvodnění 78: podporuje vhodná opatření na podporu povědomí za účelem zajištění robustních bezpečnostních postupů a dodržování politik.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21(2)(a, b): vyžaduje, aby subjekty přijaly politiky týkající se analýzy rizik a bezpečnostního školení pro veškerý relevantní personál. Tato politika tento požadavek naplňuje zavedením průběžných procesů školení citlivých na roli.

11.5.2 Článek 21(3): podporuje zvyšování povědomí o rizicích kybernetické bezpečnosti mezi vedením a zaměstnanci prostřednictvím iniciativ na podporu povědomí a simulací.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 13 – Strategie digitální provozní odolnosti: vyžaduje, aby povědomí o rizicích ICT a školení byly součástí modelu správy. Tato politika zajišťuje, že rizika související s lidským faktorem jsou řešena prostřednictvím průběžného vzdělávání a simulací hrozeb.

11.6.2 Články 5 a 8: zdůrazňují význam rámců vnitřní kontroly, jejichž základními součástmi pro odolnost ICT a kybernetickou hygienu jsou právě povědomí a školení.

11.7 COBIT 2019

11.7.1 APO07 – Řízené lidské zdroje: zdůrazňuje potřebu rozvíjet povědomí o bezpečnostních odpovědnostech a začlenit je do řízení pracovních sil.

11.7.2 DSS05 – Řízené bezpečnostní služby: stanoví opatření pro vzdělávání uživatelů a hlášení incidentů, přičemž obě oblasti jsou nedílnou součástí této politiky.

11.7.3 MEA03 – Monitorování, hodnocení a posuzování souladu: vyžaduje přezkum účinnosti chování uživatelů a dodržování politik, který je zde realizován prostřednictvím phishingových testů, kvízů a metrik kampaní na podporu povědomí.