					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P37S					Název dokumentu: **Politika právního a regulatorního souladu**							
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

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	Kapitoly 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Opatření 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
GDPR	Články 5, 6, 32, 33	
směrnice NIS2	Články 21(2)(a), 21(2)(f), 23	
nařízení DORA	Články 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Účel

1.1 Tato politika stanoví přístup organizace k identifikaci, plnění a prokazování souladu s právními, regulatorními a smluvními povinnostmi.

1.2 Stanoví jasné odpovědnosti a praktické kroky, které pomáhají společnosti plnit povinnosti v oblasti souladu, včetně požadavků na ochranu osobních údajů, rámců kybernetické bezpečnosti, smluv se zákazníky a certifikačních požadavků.

1.3 Zajišťuje, že i bez specializovaného compliance týmu může společnost udržovat právně obhajitelný provoz, přiměřeně reagovat na incidenty a zachovávat připravenost na audit.

1.4 Tato politika je nezbytná pro podporu certifikace podle ISO/IEC 27001:2022 a pro splnění externích očekávání zákazníků, regulatorních orgánů nebo partnerů.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny zaměstnance, smluvní pracovníky, freelancery a dodavatele třetích stran,

2.1.2 všechny služby, činnosti, systémy a aktivity zpracování dat, při nichž je organizace povinna plnit právní nebo smluvní požadavky,

2.1.3 všechna místa a prostředí používaná ke zpracování podnikových informací, a to v kanceláři, při práci na dálku i v cloudu.

2.2 Tato politika pokrývá:

2.2.1 předpisy o ochraně osobních údajů, jako je GDPR,

2.2.2 předpisy v oblasti kybernetické bezpečnosti, jako je směrnice NIS2,

2.2.3 povinnosti specifické pro odvětví, je-li to relevantní,

2.2.4 smlouvy se zákazníky, dohody o mlčenlivosti a auditní doložky,

2.2.5 dobrovolné certifikace (např. ISO 27001) a interní politiky, které musí být uplatňovány za účelem zajištění souladu.

3. Cíle

3.1 Stanovit odpovědnost: přiřadit jednoznačnou odpovědnost za monitorování, aktualizaci a uplatňování právních, regulatorních a smluvních povinností.

3.2 Chránit společnost: minimalizovat riziko porušení právních povinností, sankcí, bezpečnostních incidentů a poškození dobrého jména.

3.3 Zajistit připravenost na audit: uchovávat ověřitelné záznamy prokazující, jak organizace plní své povinnosti v oblasti souladu.

3.4 Podpořit integraci politik: zajistit, aby právní a regulatorní povinnosti byly důsledně promítnuty do všech politik a procesů.

3.5 Řídit výjimky transparentně: zajistit, aby veškeré výjimky ze souladu byly zdokumentovány, odůvodněny a schváleny tak, aby se předcházelo odpovědnosti.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Nese celkovou odpovědnost za právní a regulatorní soulad organizace.

4.1.2 Vede Registr souladu a zajišťuje jeho průběžnou aktuálnost.

4.1.3 Přezkoumává smlouvy se zákazníky a zajišťuje sledování a uplatňování konkrétních povinností.

4.1.4 Schvaluje výjimky z povinností v oblasti souladu pouze tehdy, jsou-li právně odůvodnitelné a jsou-li zavedena kompenzační opatření.

4.2 Externí poradci (např. právní, IT nebo compliance konzultanti)

4.2.1 Podporují GM při identifikaci použitelných právních předpisů, certifikací a povinností (např. GDPR, NIS2, ISO 27001).

4.2.2 Poskytují doporučení k výkladu nových regulatorních požadavků nebo změn stávajících právních předpisů.

4.2.3 Mohou pomáhat s aktualizací politik, audity nebo reakcí na bezpečnostní incidenty, pokud existuje právní expozice.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Plánovaný každoroční přezkum

9.1.1 Tato politika musí být každých 12 měsíců přezkoumána GM.

9.1.2 Přezkum musí potvrdit:

9.1.2.1 relevanci vůči aktuálnímu právnímu a smluvnímu kontextu,

9.1.2.2 správné promítnutí zákaznických smluv a povinností poskytování služeb,

9.1.2.3 soulad s Registrem souladu a dalšími politikami.

9.2 Aktualizace řízené událostí

9.2.1 Okamžitý přezkum je vyžadován, pokud:

9.2.1.1 se stane použitelným nový právní předpis nebo regulace (např. nové pravidlo ochrany osobních údajů),

9.2.1.2 zákazník doplní do smlouvy komplexní požadavky v oblasti souladu,

9.2.1.3 dojde k porušení zabezpečení nebo incidentu nesouladu,

9.2.1.4 společnost vstoupí na regulovaný trh nebo do regulovaného odvětví.

9.3 Schvalování aktualizací a správa verzí

9.3.1 Všechny aktualizace musí být zdokumentovány, verzovány a schváleny GM.

9.3.2 Historické verze musí být uchovávány pro účely auditu a právní účely.

9.4 Komunikace změn

9.4.1 Zaměstnanci a smluvní pracovníci musí být o změnách politiky informováni do 5 pracovních dnů od schválení.

9.4.2 Všichni dotčení dodavatelé musí před pokračováním v poskytování služby rovněž potvrdit aktualizované podmínky.

10. Související politiky a vazby

10.1 Tato politika je podporována a uplatňována prostřednictvím následujících SME politik:

10.1.1 P3S – Zásady přípustného užívání: předcházejí jednání, které může porušit právní nebo smluvní podmínky (např. neoprávněné sdílení souborů).

10.1.2 P8S – Politika bezpečnostního povědomí a školení: školí personál o povinnostech v oblasti souladu a o tom, jak předcházet porušením.

10.1.3 P14S – Politika uchovávání údajů: zajišťuje zákonné postupy nakládání s daty v celém jejich životním cyklu.

10.1.4 P17S – Politika ochrany dat a soukromí: naplňuje požadavky GDPR a požadavky zákazníků na nakládání s daty.

10.1.5 P30S – Politika reakce na incidenty: stanoví postup reakce na porušení zabezpečení dat nebo selhání v oblasti souladu, včetně oznamovacích lhůt.

10.1.6 P36S – Politika sociálních médií a externí komunikace: zajišťuje, aby veřejná komunikace neporušovala právní ani regulatorní povinnosti.

10.2 Každá navázaná politika uplatňuje část rámce právního souladu a musí být používána společně s ostatními.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – Opatření k řešení rizik a příležitostí: zahrnuje rizika v oblasti souladu.

11.1.2 Kapitola 8.1 – Operativní plánování a řízení: vyžaduje provádění procesů, které splňují právní a smluvní požadavky.

11.2 ISO/IEC 27002

11.2.1 Opatření 5.36 – poskytuje organizaci vodítko pro vedení záznamů o povinnostech a zajištění odpovídajících reakcí na právní a regulatorní požadavky.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika a postupy: vyžaduje formální politiky v oblasti souladu.

11.3.2 PM-1 – Plán programu bezpečnosti informací: vyžaduje začlenění právního souladu do bezpečnostního plánování.

11.3.3 CA-1 – Hodnocení, autorizace a monitorování.

11.3.4 AU-1 – Auditní politika: vyžaduje uchovávání důkazů o souladu.

11.4 GDPR

11.4.1 Článek 5 – Zásady zpracování osobních údajů, včetně odpovědnosti.

11.4.2 Článek 6 – právní základ zpracování.

11.4.3 Článek 32 – Zabezpečení zpracování.

11.4.4 Článek 33 – Oznámení porušení zabezpečení do 72 hodin.

11.5 směrnice NIS2

11.5.1 Článek 21(2)(a) a (f) – interní politiky pro řízení rizik a regulatorní kontrolu.

11.5.2 Článek 23 – prosazování a sankce při selhání v oblasti souladu.

11.6 nařízení DORA

11.6.1 Článek 5(2) – dohled nad řízením rizik v oblasti ICT.

11.6.2 Článek 9(1) – interní správa souladu.

11.6.3 Článek 17 – smluvní ujednání s poskytovateli služeb v oblasti ICT.

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: zajišťuje, že rizika v oblasti souladu jsou sledována a řešena.

11.7.2 APO13 – Managed Security: pokrývá uplatňování regulatorního a smluvního souladu na základě rizik.

11.7.3 DSS01 – Managed Operations: vyžaduje provozní připravenost k plnění právních povinností.