| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vložte název registrované právnické osoby | | | | | | | |
| Číslo dokumentu:<br>P37 | | | | | Název dokumentu:<br>**Politika právního a regulatorního souladu** | | | | | | | |
| Verze:<br>1.0 | | Datum účinnosti:<br>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** |
| | | | |
| | | | |

## 1. Účel

1.1 Tato politika stanoví závazný rámec pro identifikaci, řízení a zajištění souladu se všemi právními, regulatorními a smluvními povinnostmi relevantními pro bezpečnost informací, ochranu osobních údajů a provozní činnosti organizace.

1.2 Cílem je předcházet nesouladu, který by mohl vést k pokutám, právní odpovědnosti, narušení činnosti, poškození dobrého jména nebo regulatornímu zásahu.

1.3 Tato politika podporuje začlenění požadavků na soulad do správy a řízení, řízení rizik, provozních postupů, životního cyklu projektů a návrhu systémů.

1.4 Zajišťuje, aby všechny relevantní povinnosti napříč jurisdikcemi, odvětvími a regulatorními rámci byly v organizaci jednoznačně dokumentovány, posouzeny, monitorovány a uplatňovány.

## 2. Rozsah

**2.1 Tato politika se vztahuje na všechna oddělení, funkce, organizační útvary a osoby jednající jménem organizace, včetně:**

2.1.1 zaměstnanců v trvalém i dočasném pracovním poměru,

2.1.2 dodavatelů, konzultantů a stážistů,

2.1.3 dodavatelů, zpracovatelů nebo partnerů třetích stran, kteří nakládají s daty, systémy nebo regulatorními povinnostmi organizace,

2.1.4 veškerých podnikových procesů, projektů nebo iniciativ podléhajících právnímu nebo regulatornímu dohledu.

**2.2 Oblasti souladu upravené touto politikou zahrnují mimo jiné:**

2.2.1 povinnosti v oblasti informační a kybernetické bezpečnosti (např. ISO/IEC 27001, NIS2, DORA),

2.2.2 právní předpisy v oblasti ochrany osobních údajů a soukromí (např. GDPR, odvětvové právní předpisy na ochranu soukromí),

2.2.3 odvětvové regulace (např. finanční, zdravotnické, automobilové, obranné),

2.2.4 smluvní povinnosti vyplývající z dohod o mlčenlivosti, dohod o úrovni služeb (SLA) nebo smluv o zpracování uzavřených s třetími stranami,

2.2.5 právní požadavky související s hlášením incidentů, součinností s orgány činnými v trestním řízení a mezinárodními přenosy dat.

## 3. Cíle

3.1 Zajistit, aby všechny použitelné zákony, právní předpisy, normy a smluvní povinnosti byly v celé organizaci identifikovány, dokumentovány, vyloženy a uplatňovány.

3.2 Začlenit právní a regulatorní požadavky do systému řízení bezpečnosti informací (ISMS) organizace, procesů řízení rizik, smluv s dodavateli a návrhu produktů a služeb.

3.3 Zajistit mechanismus pro proaktivní sledování regulatorních změn a odpovídající aktualizaci opatření a dokumentace.

3.4 Stanovit jasnou odpovědnost za dohled nad souladem, eskalaci porušení, řízení výjimek a externí oznamování.

3.5 Zajistit auditovatelnost a obhajitelnost právního a regulatorního postavení organizace při kontrolách, vyšetřováních nebo certifikačních přezkumech.

## 4. Role a odpovědnosti

### 4.1 Vrcholové vedení

4.1.1 Nese strategickou odpovědnost za soulad s právními a regulatorními požadavky v celé organizaci.

4.1.2 Přezkoumává a schvaluje rozhodnutí v oblasti souladu s vysokým dopadem, včetně akceptace rizik a právních sporů.

**4.2 Manažer souladu / vedoucí právního oddělení / právní zástupce**

4.2.1 Udržuje registr povinností v oblasti souladu obsahující všechny použitelné zákony, normy, certifikace a smluvní ustanovení.

4.2.2 Provádí posouzení právních dopadů nových služeb, trhů nebo toků dat.

4.2.3 Poskytuje závazný výklad právních předpisů a norem.

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

**9. Požadavky na přezkoumání a aktualizaci**

**9.1 Každoroční přezkum politiky**

**9.1.1 Tato politika musí být přezkoumána nejméně jednou za kalendářní rok za účelem:**

9.1.1.1 zajištění trvalého souladu s aktualizovanými právními předpisy, oborovými normami a regulatorními rámci,

9.1.1.2 ověření provozní účinnosti na základě auditních zjištění a historie incidentů,

9.1.1.3 promítnutí změn v organizaci (např. nové jurisdikce, systémy nebo oblasti podnikání).

**9.2 Přezkumy vyvolané událostí**

9.2.1 Mimořádné přezkumy musí být zahájeny, pokud:

9.2.2 je přijat nebo aktualizován nový právní nebo regulatorní požadavek,

9.2.3 incident v oblasti souladu nebo audit odhalí nedostatky politiky,

9.2.4 organizace vstoupí na nový trh nebo do nové oblasti služeb řízené odlišnými rámci souladu,

9.2.5 trendy v prosazování nebo pokyny regulatorních orgánů signalizují změnu postoje k riziku.

**9.3 Vlastnictví a schvalování**

9.3.1 Právní oddělení a manažer souladu nesou společnou odpovědnost za koordinaci procesu přezkumu.

9.3.2 Konečné změny politiky musí schválit vrcholové vedení a musí být zaznamenány v registru změn politik spolu se souvisejícími odkazy na řízení změn a komunikačními plány.

**9.4 Správa verzí a komunikace**

**9.4.1 Jakákoli aktualizovaná verze této politiky musí:**

9.4.1.1 obsahovat shrnutí klíčových změn,

9.4.1.2 být znovu distribuována prostřednictvím oficiálních kanálů (např. portál politik, LMS, interní zpravodaje),

9.4.1.3 vyžadovat potvrzení seznámení od dotčených pracovníků, zejména těch v právních, provozních, bezpečnostních a dodavatelských rolích.

**10. Související politiky a vazby**

**10.1 Tato politika se uplatňuje společně s následujícími politikami v rámci ISMS organizace a posiluje je:**

10.1.1 P1 – Politika informační bezpečnosti: stanoví základní principy správy a řízení, které zajišťují, aby všechny politiky informační bezpečnosti včetně požadavků na soulad byly v souladu se strategickými obchodními a regulatorními požadavky.

10.1.2 P2 – Politika rolí a odpovědností v oblasti správy a řízení: vymezuje rozhodovací pravomoci včetně právních a compliance rolí odpovědných za regulatorní dohled a odpovědnost.

10.1.3 P6 – Politika řízení rizik: podporuje hodnocení, vlastnictví a mitigaci rizik právního a regulatorního souladu v celé organizaci.

10.1.4 P8 – Politika povědomí o informační bezpečnosti a školení: zajišťuje, aby byl veškerý personál informován o povinnostech v oblasti souladu a absolvoval školení odpovídající jeho roli.

10.1.5 P12 – Politika správy aktiv: posiluje právní povinnosti při správě a ochraně regulovaných nebo smluvně vázaných aktiv, včetně aktiv zahrnujících osobní údaje a kritickou infrastrukturu.

10.1.6 P30 – Politika reakce na incidenty (P30): upravuje povinná právní oznámení (např. článek 33 GDPR) a eskalační postupy v případě porušení souladu nebo regulatorní události.

10.1.7 P33 – Politika monitorování auditu a souladu: poskytuje strukturované činnosti zajištění, včetně testování opatření a shromažďování důkazů, požadované pro interní a externí ověření souladu.

## 11. Referenční normy a rámce

### 11.1 ISO/IEC 27001

11.1.1 Kapitola 4.2 – Porozumění potřebám a očekáváním zainteresovaných stran: vyžaduje identifikaci a začlenění právních a regulatorních požadavků do ISMS.

11.1.2 Kapitola 5.1 – Vedení a závazek: stanoví odpovědnost vrcholového vedení za nastavení a udržování právního souladu v celé organizaci.

11.1.3 Kapitola 5.3 – Organizační role, odpovědnosti a pravomoci: zajišťuje jasné vymezení rolí pro právní dohled a regulatorní soulad.

11.1.4 Příloha A, opatření 5.36 – Soulad s právními a smluvními požadavky: stanoví požadavek identifikovat a plnit povinnosti vyplývající ze zákonů, právních předpisů a smluv.

### 11.2 ISO/IEC 27002

11.2.1 Opatření 5.36: uvádí implementační pokyny pro vedení registru povinností v oblasti souladu, ověřování regulatorních požadavků a zajištění strukturovaného uchovávání důkazů.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika a postupy bezpečnostního plánování: vyžaduje, aby požadavky na soulad byly začleněny do struktur správy a řízení a dokumentace.

11.3.2 PM-1 – Plán programu bezpečnosti informací: stanoví regulatorní opatření jako součást širšího bezpečnostního programu.

11.3.3 CA-7 – Průběžné monitorování: podporuje dohled nad účinností opatření při plnění právních požadavků a požadavků politik.

11.3.4 AU-9 – Ochrana auditních informací: zajišťuje, aby auditní logy a záznamy o souladu byly chráněny a dostupné pro kontrolu.

### 11.4 GDPR / obecné nařízení o ochraně osobních údajů (2016/679)

11.4.1 Článek 5 – Zásady zpracování osobních údajů: vyžaduje zákonnost zpracování, transparentnost a odpovědnost.

11.4.2 Článek 6 – Zákonnost zpracování: stanoví odpovídající právní základy pro všechny činnosti zpracování dat.

11.4.3 Článek 24 – Odpovědnost správce: zakládá přímou odpovědnost za zajištění regulatorního souladu.

11.4.4 Článek 32 – Zabezpečení zpracování: vyžaduje zavedení odpovídajících technických a organizačních opatření (TOM).

11.4.5 Článek 33 – Oznámení porušení zabezpečení: vyžaduje, aby porušení zabezpečení osobních údajů byla oznámena příslušným orgánům do 72 hodin.

### 11.5 Směrnice NIS2 (2022/2555)

11.5.1 Články 20–21: vyžadují, aby základní a důležité subjekty zavedly dokumentovanou správu a řízení, strategie právního souladu a průběžný přezkum právních rizik.

**11.6 Nařízení DORA (2022/2554)**

11.6.1 Článek 5(2) – Řízení rizik v oblasti ICT: vyžaduje začlenění právního souladu do širších funkcí řízení rizik a dohledu.

11.6.2 Článek 19 – Rizika ICT třetích stran: ukládá specifické právní požadavky pro řízení smluvních a regulatorních povinností zahrnujících externí dodavatele a platformy.

**11.7 COBIT 2019**

11.7.1 APO12 – Řízení rizik: zahrnuje právní a regulatorní soulad jako kritické součásti podnikové správy rizik.

11.7.2 MEA03 – Monitorovat, vyhodnocovat a posuzovat soulad s externími požadavky: vymezuje průběžné monitorování, řízení výjimek a připravenost na audit pro všechny formy regulatorních povinností.