					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P37					Názov dokumentu: **Politika právneho a regulačného súladu**							
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**

1. Účel

1.1 Táto politika stanovuje záväzný rámec na identifikáciu, riadenie a zabezpečenie súladu so všetkými právnymi, regulačnými a zmluvnými povinnosťami relevantnými pre informačnú bezpečnosť organizácie, ochranu údajov a prevádzkové činnosti.

1.2 Cieľom je predchádzať nesúladu, ktorý by mohol viesť k pokutám, právnej zodpovednosti, narušeniu činnosti organizácie, reputačnej ujme alebo zásahu regulačných orgánov.

1.3 Táto politika podporuje integráciu požiadaviek na súlad do správy a riadenia, riadenia rizík, prevádzkových procesov, životného cyklu projektov a návrhu systémov.

1.4 Zabezpečuje, aby všetky relevantné povinnosti v rôznych jurisdikciách, odvetviach a regulačných rámcoch boli v organizácii jednoznačne zdokumentované, posúdené, monitorované a uplatňované.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky oddelenia, funkcie, organizačné jednotky a osoby konajúce v mene organizácie vrátane:

2.1.1 stálych a dočasných zamestnancov,

2.1.2 zmluvných pracovníkov, konzultantov a stážistov,

2.1.3 dodávateľov tretích strán, sprostredkovateľov spracúvania alebo partnerov, ktorí nakladajú s údajmi, systémami alebo regulačnými povinnosťami organizácie,

2.1.4 akéhokoľvek podnikového procesu, projektu alebo iniciatívy podliehajúcich právnemu alebo regulačnému dohľadu.

2.2 Oblasti súladu upravené touto politikou zahŕňajú okrem iného:

2.2.1 povinnosti v oblasti informačnej a kybernetickej bezpečnosti (napr. ISO/IEC 27001, NIS2, DORA),

2.2.2 právne predpisy v oblasti ochrany osobných údajov a súkromia (napr. GDPR, odvetvové právne predpisy o ochrane súkromia),

2.2.3 odvetvové predpisy (napr. finančné, zdravotnícke, automobilové, obranné),

2.2.4 zmluvné povinnosti vyplývajúce z dohôd o mlčanlivosti, dohôd o úrovni služieb (SLA) alebo zmlúv o spracúvaní údajov s tretími stranami,

2.2.5 zákonné požiadavky súvisiace s nahlasovaním incidentov, komunikáciou s orgánmi činnými v trestnom konaní a medzinárodným prenosom údajov.

3. Ciele

3.1 Zabezpečiť, aby všetky uplatniteľné zákony, predpisy, normy a zmluvné povinnosti boli v rámci organizácie identifikované, zdokumentované, interpretované a uplatňované.

3.2 Integrovať právne a regulačné požiadavky do systému manažérstva informačnej bezpečnosti (ISMS), procesov riadenia rizík, zmlúv s dodávateľmi a návrhu produktov a služieb organizácie.

3.3 Zaviesť mechanizmus na proaktívne monitorovanie regulačných zmien a zodpovedajúcu aktualizáciu kontrol a dokumentácie.

3.4 Vymedziť jasné priradenie zodpovednosti za dohľad nad súladom, eskaláciu porušení, riešenie výnimiek a externé oznamovanie.

3.5 Zabezpečiť auditovateľnosť a obhájiteľnosť právneho a regulačného postavenia organizácie počas inšpekcií, vyšetrovaní alebo certifikačných preskúmaní.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Nesie strategickú zodpovednosť za zabezpečenie súladu s právnymi a regulačnými požiadavkami v celej organizácii.

4.1.2 Preskúmava a schvaľuje rozhodnutia o súlade s vysokým rizikom vrátane akceptácie rizika a právnych sporov.

4.2 Compliance officer / generálny právnik / právny poradca

4.2.1 Vedie register povinností súladu, ktorý obsahuje všetky uplatniteľné zákony, normy, certifikácie a zmluvné ustanovenia.

4.2.2 Vykonáva posúdenia právnych dopadov pre nové služby, trhy alebo toky údajov.

4.2.3 Poskytuje záväzný výklad zákonov a noriem.

[... 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 politiky

9.1.1 Táto politika sa musí preskúmať najmenej raz za kalendárny rok s cieľom:

9.1.1.1 zabezpečiť trvalý súlad s aktualizovanými zákonmi, odvetvovými normami a regulačnými rámcami,

9.1.1.2 overiť prevádzkovú účinnosť na základe auditných zistení a histórie incidentov,

9.1.1.3 zohľadniť organizačné zmeny (napr. nové jurisdikcie, systémy alebo oblasti podnikania).

9.2 Preskúmania na základe spúšťacích udalostí

9.2.1 Medzobdobné preskúmania sa musia vykonať, ak:

9.2.2 je prijatá alebo aktualizovaná nová právna alebo regulačná požiadavka,

9.2.3 incident súvisiaci so súladom alebo audit odhalí nedostatky politiky,

9.2.4 organizácia vstúpi na nový trh alebo do novej oblasti služieb riadenej odlišnými rámcami súladu,

9.2.5 trendy v presadzovaní predpisov alebo usmernenia regulátorov naznačujú zmenu rizikového profilu.

9.3 Vlastníctvo a schvaľovanie

9.3.1 Právne oddelenie a compliance officer nesú spoločnú zodpovednosť za koordináciu procesu preskúmania.

9.3.2 Konečné revízie politiky musia byť schválené vrcholovým manažmentom a zaznamenané v registri zmien politík spolu so súvisiacimi odkazmi na riadenie zmien a komunikačnými plánmi.

9.4 Riadenie verzií a komunikácia

9.4.1 Každá aktualizovaná verzia tejto politiky musí:

9.4.1.1 obsahovať súhrn kľúčových zmien,

9.4.1.2 byť opätovne distribuovaná prostredníctvom oficiálnych kanálov (napr. portál politík, LMS, interné bulletiny),

9.4.1.3 vyžadovať potvrdenie oboznámenia sa od dotknutých pracovníkov, najmä v právnych, prevádzkových, bezpečnostných rolách a rolách riadenia dodávateľov.

10. Súvisiace politiky a väzby

10.1 Táto politika sa uplatňuje spolu s nasledujúcimi politikami v rámci ISMS organizácie a posilňuje ich:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje základné princípy správy a riadenia, ktoré zabezpečujú, aby všetky politiky informačnej bezpečnosti vrátane oblasti súladu boli zosúladené so strategickými požiadavkami organizácie a regulačnými požiadavkami.

10.1.2 P2 – Politika rolí a zodpovedností v oblasti správy a riadenia: vymedzuje rozhodovacie právomoci vrátane právnych a compliance rolí zodpovedných za regulačný dohľad a priradenie zodpovednosti.

10.1.3 P6 – Politika riadenia rizík: podporuje hodnotenie, vlastníctvo a zmierňovanie rizík právneho a regulačného súladu v celej organizácii.

10.1.4 P8 – Politika povedomia a školení v oblasti informačnej bezpečnosti: zabezpečuje, aby všetci pracovníci boli informovaní o povinnostiach súladu a absolvovali školenia primerané svojej role.

10.1.5 P12 – Politika správy aktív: posilňuje právne povinnosti pri riadení a ochrane regulovaných alebo zmluvných aktív vrátane aktív súvisiacich s osobnými údajmi a kritickou infraštruktúrou.

10.1.6 P30 – Politika reakcie na incidenty (P30): upravuje povinné právne oznámenia (napr. článok 33 GDPR) a eskalačné postupy v prípade porušenia súladu alebo regulačnej udalosti.

10.1.7 P33 – Politika monitorovania auditu a súladu: poskytuje štruktúrované uisťovacie činnosti vrátane testovania kontrol a zhromažďovania dôkazov, ktoré sa vyžadujú na interné a externé overovanie súladu.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 4.2 – Pochopenie potrieb a očakávaní zainteresovaných strán: vyžaduje identifikáciu a integráciu právnych a regulačných požiadaviek do ISMS.

11.1.2 Kapitola 5.1 – Vodcovstvo a záväzok: vyžaduje zodpovednosť vrcholového vedenia za zavedenie a udržiavanie právneho súladu v celej organizácii.

11.1.3 Kapitola 5.3 – Organizačné roly, zodpovednosti a právomoci: zabezpečuje jednoznačné vymedzenie rolí pre právny dohľad a regulačný súlad.

11.1.4 Príloha A Kontrola 5.36 – Súlad s právnymi a zmluvnými požiadavkami: stanovuje požiadavku identifikovať a plniť povinnosti vyplývajúce zo zákonov, predpisov a zmlúv.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.36: podrobne upravuje implementačné usmernenia na vedenie registra povinností súladu, overovanie regulačných požiadaviek a zabezpečenie štruktúrovaného uchovávania dôkazov.

11.3 NIST SP 800-53 Rev.

11.3.1 PL-1 – Politika a postupy bezpečnostného plánovania: vyžaduje, aby požiadavky na súlad boli integrované do štruktúr správy a riadenia a dokumentácie.

11.3.2 PM-1 – Plán programu informačnej bezpečnosti: stanovuje regulačné kontroly ako súčasť širšieho bezpečnostného programu.

11.3.3 CA-7 – Nepretržité monitorovanie: podporuje dohľad nad účinnosťou kontrol pri plnení právnych požiadaviek a požiadaviek politík.

11.3.4 AU-9 – Ochrana auditných informácií: zabezpečuje, aby auditné logy a záznamy o súlade boli chránené a dostupné na kontrolu.

11.4 GDPR EÚ (2016/679)

11.4.1 Článok 5 – Zásady spracúvania: vyžaduje zákonné spracúvanie, transparentnosť a zodpovednosť.

11.4.2 Článok 6 – Zákonnosť spracúvania: stanovuje požiadavku na primerané právne základy pre všetky činnosti spracúvania údajov.

11.4.3 Článok 24 – Zodpovednosť prevádzkovateľa: ustanovuje priamu zodpovednosť za zabezpečenie regulačného súladu.

11.4.4 Článok 32 – Bezpečnosť spracúvania: vyžaduje zavedenie primeraných technických a organizačných opatrení.

11.4.5 Článok 33 – Oznamovanie porušenia ochrany údajov: vyžaduje, aby porušenia ochrany osobných údajov boli nahlásené príslušným orgánom do 72 hodín.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Články 20–21: vyžadujú, aby základné a dôležité subjekty zaviedli zdokumentovanú správu a riadenie, stratégie právneho súladu a nepretržité preskúmavanie právnych rizík.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 5(2) – Rámec riadenia rizík IKT: vyžaduje integráciu právneho súladu do širších funkcií riadenia rizík a dohľadu.

11.6.2 Článok 19 – Riziko tretích strán v oblasti IKT: ukladá osobitné právne požiadavky na riadenie zmluvných a regulačných povinností týkajúcich sa externých dodávateľov a platforiem.

11.7 COBIT 2019

11.7.1 APO12 – Riadenie rizík: zahŕňa právny a regulačný súlad ako kritické súčasti podnikovej správy a riadenia rizík.

11.7.2 MEA03 – Monitorovanie súladu s externými požiadavkami: vymedzuje priebežné monitorovanie, riadenie výnimiek a pripravenosť na audit pre všetky formy regulačných povinností.