					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P33					Názov dokumentu: **Politika monitorovania auditov a 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**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 9.2, 9.3, 10	
ISO/IEC 27002:2022	Kontroly 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
Nariadenie EÚ GDPR	Články 24, 32, 33	
Smernica EÚ NIS2	Článok 21(2)(g), 27	
Nariadenie EÚ DORA	Články 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Účel

1.1 Účelom tejto politiky je stanoviť a riadiť program monitorovania auditov a súladu v organizácii tak, aby:

1.1.1 overoval účinnosť bezpečnostných kontrol a kontrol ochrany súkromia,

1.1.2 zabezpečoval súlad s príslušnými normami, právnymi rámcami a zmluvnými záväzkami,

1.1.3 včas identifikoval nezhody, neefektívnosti a riziká nesúladu,

1.1.4 podporoval neustále zlepšovanie a pripravenosť na certifikácie, posúdenia a regulačné preskúmania.

1.2 Táto politika podporuje integritu a vyspelosť systému manažérstva informačnej bezpečnosti (ISMS) zavedením štruktúrovaných auditných a monitorovacích postupov založených na dôkazoch a orientovaných na riziká.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky:

2.1.1 interné organizačné jednotky, funkcie a oddelenia,

2.1.2 fyzické priestory, cloudové prostredia, platformy SaaS a outsourcované služby,

2.1.3 informačné systémy, aplikácie, infraštruktúru a dátové aktíva spravované v rámci ISMS,

2.1.4 zamestnancov, dodávateľov a poskytovateľov služieb tretích strán, ktorí majú povinnosti v oblasti auditu alebo súladu.

2.2 Politika sa vzťahuje na:

2.2.1 interné audity,

2.2.2 externé a certifikačné audity,

2.2.3 technické monitorovanie súladu,

2.2.4 audity dodávateľov a tretích strán,

2.2.5 nápravné a preventívne opatrenia (CAPA),

2.2.6 metriky, dashboardy a procesy reportovania.

2.3 Vzťahuje sa na všetky relevantné rámce, ktorým organizácia podlieha, vrátane ISO/IEC 27001, GDPR, NIS2, DORA a SOC 2.

3. Ciele

3.1 Overovať primeranosť a účinnosť zavedených kontrol, politík a postupov v rámci ISMS a súvisiacich prostredí.

3.2 Identifikovať a odstrániť nedostatky, nezhody alebo medzery v súlade skôr, ako prerastú do incidentov alebo porušení povinností.

3.3 Zabezpečovať priebežnú pripravenosť na interné preskúmania manažmentom, externé audity a nezávislé certifikácie.

3.4 Vytvárať obhájiteľné dôkazy a auditné stopy na podporu regulačných šetrení, právnych konaní alebo požiadaviek zákazníkov na preukázanie uistenia.

3.5 Integrovať výsledky auditov do širšieho rámca riadenia rizík, bezpečnostných metrík a aktivít neustáleho zlepšovania organizácie.

4. Roly a zodpovednosti

4.1 Vedúci interného auditu / manažér súladu

4.1.1 Plánuje, harmonogramuje a vykonáva interné audity na základe rizikových priorít.

4.1.2 Vedie register auditov, koordinuje auditné činnosti a sleduje plnenie nápravných opatrení.

4.2 Riaditeľ informačnej bezpečnosti (CISO)

4.2.1 Zabezpečuje, aby rozsah auditu zahŕňal všetky relevantné prvky ISMS a kontroly prílohy A.

4.2.2 Dohliada na overovanie CAPA a integruje výsledky auditov do bezpečnostného programu.

[... 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 Túto politiku musí manažér súladu a CISO preskúmať najmenej raz ročne alebo skôr v reakcii na:

9.1.1 zmeny regulačných, zmluvných alebo certifikačných rámcov,

9.1.2 významné auditné zistenia alebo opakované zlyhania kontrol,

9.1.3 organizačnú reštrukturalizáciu alebo zmeny systému GRC,

9.1.4 odporúčania externého audítora alebo spätnú väzbu regulátora.

9.2 V rámci preskúmania sa musí posúdiť:

9.2.1 metodika a frekvencia plánovania auditov,

9.2.2 zmeny rozsahu ISMS alebo infraštruktúry,

9.2.3 aktualizácie katalógu kontrol alebo registra právnych požiadaviek,

9.2.4 konzistentnosť a kvalita auditných dôkazov a procesov CAPA.

9.3 Všetky zmeny politiky musia byť:

9.3.1 zdokumentované v úložisku s riadením verzií,

9.3.2 schválené vrcholovým manažmentom,

9.3.3 oznámené všetkým dotknutým osobám a premietnuté do aktualizovaných postupov a programov zvyšovania povedomia.

9.4 Po preskúmaní musí validácia potvrdiť, že aktualizované požiadavky sú premietnuté do registra auditov, nástrojov na riadenie súladu a interných monitorovacích dashboardov.

10. Súvisiace politiky a väzby

10.1 Táto politika je zosúladená s týmito súvisiacimi politikami organizácie:

10.1.1 P1 – Politika informačnej bezpečnosti: Definuje ISMS a stanovuje zodpovednosť za súlad a neustále zlepšovanie.

10.1.2 P5 – Politika riadenia zmien: Zabezpečuje viditeľnosť auditov nad zmenami infraštruktúry a konfigurácie, ktoré ovplyvňujú kontrolné prostredie.

10.1.3 P6 – Politika riadenia rizík: Integruje výstupy auditov do hodnotenia podnikových rizík a činností ich ošetrenia.

10.1.4 P14 – Politika uchovávania a likvidácie údajov: Upravuje uchovávanie auditných dôkazov, logov a záznamov o súlade.

10.1.5 P18 – Politika kryptografických kontrol: Podporuje bezpečné ukladanie a prenos citlivých auditných údajov.

10.1.6 P26 – Politika bezpečnosti tretích strán a dodávateľov: Pokrýva práva na audit, dokumentáciu uistenia a dohľad nad súladom dodávateľov.

10.1.7 P30 – Politika reakcie na incidenty: Zosúlaďuje audity procesov riešenia incidentov s cieľmi uistenia v rámci ISMS.

10.1.8 P32 – Politika kontinuity činností a obnovy po havárii: Vyžaduje overenie testovania kontinuity a súladu s DRP počas auditných cyklov.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s globálnymi normami a právnymi požiadavkami na audit a priebežné overovanie súladu.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 9.2 – Interný audit: Vyžaduje pravidelné interné audity ISMS založené na rizikách na vyhodnotenie účinnosti a súladu.

11.2.2 Kapitola 9.3 – Preskúmanie manažmentom: Výstupy auditov musia byť vstupom do strategického preskúmania a zlepšovania.

11.2.3 Kapitola 10.1 – Nezhoda a nápravné opatrenie: Auditné zistenia sa musia riešiť prostredníctvom zdokumentovaných postupov CAPA.

11.3 ISO/IEC 27002:2022 – Kontroly 5.35–5.37:

11.3.1 Kontroly prílohy A 5.35–5.37: Pokrývajú nezávislé preskúmanie, súlad s právnymi a zmluvnými požiadavkami a auditné logovanie.

11.3.2 Poskytujú implementačné usmernenia na plánovanie, vykonávanie a zlepšovanie auditných programov a programov monitorovania súladu.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Posúdenia kontrol: Vyžaduje rutinné preskúmavanie zavedených bezpečnostných kontrol.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): Je v súlade so sledovaním a odstraňovaním auditných zistení.

11.4.3 CA-7 – Priebežné monitorovanie: Podporuje proaktívne a automatizované posudzovanie súladu.

11.5 Nariadenie EÚ GDPR (2016/679):

11.5.1 Články 24 a 32: Vyžadujú dôkazy o zavedení a účinnosti bezpečnostných kontrol prostredníctvom primeraných riadiacich štruktúr.

11.5.2 Článok 33: Podporuje potrebu overených auditných stôp pri riešení narušenia bezpečnosti a oznamovaní.

11.6 Smernica EÚ NIS2 (2022/2555):

11.6.1 Článok 21(2)(g): Vyžaduje auditovanie politík a postupov ako súčasť minimálnych opatrení riadenia kybernetických rizík.

11.6.2 Článok 27: Národné orgány môžu vykonávať audity alebo ich vyžadovať pre základné a dôležité subjekty.

11.7 Nariadenie EÚ DORA (2022/2554):

11.7.1 Článok 10(2)(e): Subjekty musia vykonávať interné a externé audity postupov riadenia IKT rizík.

11.7.2 Článok 25 – Požiadavky na audit: Ukladá pravidelné audity vykonávané internými alebo nezávislými externými audítormi s regulačnou dohľadateľnosťou.

11.8 COBIT 2019:

11.8.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Zabezpečuje, aby sa účinnosť kontrol overovala a reportovala riadiacim orgánom.

11.8.2 MEA03 – Monitor, Evaluate and Assess Compliance: Vyžaduje zosúladenie organizačných postupov s právnymi, zmluvnými a normatívnymi požiadavkami.