					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P33S					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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 9.2, 10	Interné audity, nepretržité zlepšovanie a náprava nesúladov
ISO/IEC 27002:2022	Kontroly 5.35, 5.37	Plánované interné preskúmania, nezávislé preskúmania outsourcovaných procesov
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Bezpečnostné posúdenia, nepretržité monitorovanie, preskúmanie, analýza a vykazovanie auditov
GDPR EÚ	Články 24 a 32	Audit technických a organizačných opatrení (TOM) a dôkazy o účinnosti kontrol
Smernica EÚ NIS2	Článok 21(2)(f)	Proaktívne preskúmanie a súlad založený na dôkazoch
Nariadenie EÚ DORA	Článok 10	Riadenie IKT rizík, monitorovanie a vykazovanie
COBIT 2019	MEA01, MEA03	Monitorovanie a posudzovanie súladu, súlad a pripravenosť na preskúmania treťou stranou

1. Účel

1.1 Táto politika stanovuje prístup organizácie k vykonávaniu interných auditov, overovaniu bezpečnostných kontrol a monitorovaniu súladu s požiadavkami.

Zabezpečuje, aby všetky kontroly, politiky, systémy a poskytovatelia služieb podliehali pravidelnému a štruktúrovanému preskúmaniu.

1.2 Účelom je identifikovať zlyhania kontrol, predchádzať nesúladu a preukázať náležitú starostlivosť podľa ISO/IEC 27001, GDPR a súvisiacich rámcov.

1.3 Umožňuje MSP udržiavať prevádzkovú kontrolu a pripravenosť na certifikáciu aj bez samostatného oddelenia súladu, a to použitím jednoduchých, opakovateľných kontrolných zoznamov a zistení prioritizovaných podľa rizika.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky interné oddelenia a externých poskytovateľov služieb so zodpovednosťami súvisiacimi so systémami IT, osobnými údajmi a službami kritickými pre podnikanie,

2.1.2 všetky kontroly a systémy v rozsahu systému manažérstva informačnej bezpečnosti (ISMS),

2.1.3 všetky interné audity, preskúmania bezpečnostných kontrol a kontroly súladu bez ohľadu na to, či sa vykonávajú interne alebo externým konzultantom, klientom alebo regulačným orgánom.

2.2 Táto politika sa vzťahuje aj na zber dôkazov a vykazovanie pre:

2.2.1 certifikačné a recertifikačné audity ISO/IEC 27001,

2.2.2 audity ochrany údajov podľa GDPR alebo zmluvných podmienok,

2.2.3 bezpečnostné dotazníky alebo previerky due diligence iniciované klientom,

2.2.4 akékoľvek regulačné alebo nezávislé preskúmania podľa NIS2 alebo DORA (ak je to relevantné).

3. Ciele

3.1 Zabezpečiť, aby boli všetky kľúčové kontroly a politiky pravidelne preskúmavané z hľadiska účinnosti a súladu.

3.2 Udržiavať auditnú stopu a záznamy o nápravných opatreniach na preukázanie zodpovednosti a zlepšovania.

3.3 Pripraviť sa na certifikáciu, recertifikáciu a programy uistenia zákazníkov (napr. ISO 27001, onboarding dodávateľov).

3.4 Včas identifikovať medzery v kontrolách, aby bolo možné bezodkladne vykonať nápravu skôr, než dôjde k eskalácii problému alebo porušeniu povinností.

3.5 Umožniť generálnemu manažérovi (GM) a poskytovateľovi IT koordinovať preskúmania s minimálnou zložitosťou pri súčasnom zabezpečení obhájiteľných výsledkov.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 vykonáva dohľad nad programom auditov,

4.1.2 schvaľuje plány interných preskúmaní a zistenia,

4.1.3 prideľuje nápravné opatrenia a sleduje ich plnenie,

4.1.4 schvaľuje zapojenie externých audítorov alebo konzultantov.

4.2 Poskytovateľ IT / administrátor

4.2.1 poskytuje dôkazy počas interných a externých auditov (napr. logy, konfigurácie, záznamy o riadení prístupu),

4.2.2 pomáha pri technických kontrolách (napr. stav zálohovania, súlad záplatovania),

4.2.3 udržiava úložisko auditných dôkazov.

[... 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 a plánu auditov

9.1.1 Generálny manažér (GM) musí túto politiku a harmonogram auditov preskúmať najmenej raz ročne.

9.1.2 Preskúmanie musí vyhodnotiť:

9.1.2.1 účinnosť auditov pri identifikácii medzier v kontrolách,

9.1.2.2 mieru dokončenia auditov a nápravných opatrení,

9.1.2.3 zmeny v uplatniteľných právnych, regulačných alebo certifikačných požiadavkách.

9.2 Aktualizácie na základe spúšťacích udalostí

9.2.1 Politika musí byť preskúmaná a aktualizovaná, keď:

9.2.2 certifikačný alebo dozorný audit povedie k závažnému nesúladu,

9.2.3 dôjde k zmene právnych alebo regulačných rámcov (napr. nové usmernenia GDPR, národná implementácia NIS2),

9.2.4 zmeny v organizácii ovplyvnia systémy, procesy alebo dodávateľov zahrnutých do rozsahu auditu,

9.2.5 kritický incident alebo porušenie ochrany osobných údajov odhalí predtým nezistené medzery v kontrolách.

9.3 Dokumentovanie aktualizácií

9.3.1 Všetky revízie musia byť sledované v evidencii verzií politiky.

9.3.2 Aktualizácie musia byť distribuované všetkým členom tímu zapojeným do auditov.

9.3.3 Súhrn zmien musí byť priložený k aktualizovanej politike s cieľom zabezpečiť porozumenie.

10. Súvisiace politiky a väzby

10.1 Túto politiku podporujú a posilňujú viaceré ďalšie politiky MSP:

10.1.1 P1S – Politika informačnej bezpečnosti: stanovuje požiadavky referenčnej úrovne bezpečnosti pre všetky kontroly a vyžaduje ich uplatňovanie prostredníctvom auditov.

10.1.2 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: stanovuje zodpovednosť za plánovanie auditov, ich vykonávanie a vlastníctvo nápravných opatrení.

10.1.3 P6S – Politika riadenia rizík: identifikuje bezpečnostné slabiny odhalené pri auditoch a zabezpečuje, aby boli zistenia zdokumentované v registri rizík.

10.1.4 P17S – Politika ochrany údajov a súkromia: definuje kontroly GDPR, ktoré musia byť auditované, vrátane nakladania s údajmi, reakcie na porušenie ochrany údajov a oznámení o ochrane súkromia.

10.1.5 P22S – Politika logovania a monitorovania: poskytuje auditné logy a forenzné údaje používané pri preskúmaniach súladu a kontrol.

10.1.6 P30S – Politika reakcie na incidenty: vyžaduje pravidelný audit záznamov o incidentoch a poincidentných revízií na overenie účinnosti reakcie.

10.1.7 P31S – Politika zberu dôkazov a forenznej analýzy: poskytuje postupy na zhromažďovanie overiteľných dôkazov s reťazcom zverenia počas auditov.

10.2 Tieto politiky spolu vytvárajú uzavreté kontrolné prostredie, ktoré umožňuje interné overovanie, externé uistenie a správu a riadenie v súlade s normami.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Kapitola 9.2 – vyžaduje interné audity na vyhodnotenie výkonnosti ISMS a jeho súladu s požiadavkami.

11.1.2 Kapitola 10.1 – vyžaduje nepretržité zlepšovanie na základe výsledkov auditov a nápravy nesúladov.

11.2 ISO/IEC 27002:

11.2.1 Kontrola 5.35 – vyžaduje plánované interné preskúmania kontrol a procesov.

11.2.2 Kontrola 5.37 – zdôrazňuje nezávislé preskúmania, najmä pri outsourcovaných procesoch.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – bezpečnostné posúdenia: vyžaduje audity implementovaných kontrol na overenie ich účinnosti.

11.3.2 CA-7 – nepretržité monitorovanie: zdôrazňuje proaktívnu identifikáciu a preskúmanie slabín kontrol.

11.3.3 AU-6 – preskúmanie, analýza a vykazovanie auditov: vyžaduje pravidelnú analýzu auditných logov a zistení a ich riešenie.

11.4 GDPR EÚ:

11.4.1 Články 24 a 32 – vyžadujú implementáciu a audit technických a organizačných opatrení (TOM) vrátane dôkazov o účinnosti kontrol a zlepšovania v priebehu času.

11.5 Smernica EÚ NIS2 (2022/2555):

11.5.1 Články 20 – 21 – vyžadujú proaktívne preskúmanie kontrol, súlad založený na dôkazoch a auditovateľnosť pre základné a dôležité subjekty.

11.6 COBIT 2019:

11.6.1 MEA01 – Monitorovanie, hodnotenie a posudzovanie výkonnosti a súladu: vyžaduje pravidelné posudzovanie výkonnosti procesov a kontrol voči normám a cieľom.

11.6.2 MEA03 – Zabezpečenie súladu s externými požiadavkami: zameriava sa na interné monitorovanie a pripravenosť na audity tretích strán a regulačné preskúmania.