					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P33S					Název dokumentu: **Politika monitorování auditu a 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**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	Kapitoly 9.2, 10	interní audity, neustálé zlepšování a náprava neshod
ISO/IEC 27002:2022	Opatření 5.35, 5.37	plánované interní přezkumy, nezávislé přezkumy outsourcovaných procesů
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	bezpečnostní hodnocení, průběžné monitorování, přezkum, analýza a vykazování auditů
GDPR EU	Články 24 a 32	audit technických a organizačních opatření a důkazy o účinnosti kontrol
směrnice NIS2 EU	Článek 21(2)(f)	proaktivní přezkum a soulad založený na důkazech
nařízení DORA EU	Článek 10	řízení rizik v oblasti ICT, monitorování a vykazování
COBIT 2019	MEA01, MEA03	monitorování a posuzování shody, soulad, připravenost na přezkumy třetích stran

1. Účel

1.1 Tato politika stanoví přístup organizace k provádění interních auditů, kontrol bezpečnostních opatření a monitorování souladu s předpisy.

1.2 Zajišťuje, aby všechna opatření, politiky, systémy a poskytovatelé služeb podléhali pravidelnému a strukturovanému přezkumu.

1.3 Účelem je odhalovat selhání kontrol, předcházet nesouladu a prokazovat náležitou péči podle ISO/IEC 27001, GDPR a souvisejících rámců.

1.4 Umožňuje SME udržovat efektivní řízení a připravenost na certifikaci i bez specializovaného oddělení compliance, a to s využitím jednoduchých, opakovaně použitelných kontrolních seznamů souladu a zjištění prioritizovaných podle rizik.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechna interní oddělení a externí poskytovatele služeb s odpovědnostmi souvisejícími s IT systémy, osobními údaji a službami kritickými pro podnikání,

2.1.2 všechna opatření a systémy v rozsahu systému řízení bezpečnosti informací (ISMS),

2.1.3 všechny interní audity, přezkumy bezpečnostních opatření a kontroly souladu bez ohledu na to, zda jsou prováděny interně nebo externím konzultantem, klientem či regulačním orgánem.

2.2 Tato politika se dále vztahuje na shromažďování důkazů a vykazování pro:

2.2.1 certifikační a recertifikační audity ISO/IEC 27001,

2.2.2 audity ochrany osobních údajů podle GDPR nebo smluvních požadavků,

2.2.3 bezpečnostní dotazníky nebo přezkumy náležité péče vyžadované klienty,

2.2.4 jakékoli regulační nebo nezávislé přezkumy podle NIS2 nebo DORA, je-li to relevantní.

3. Cíle

3.1 Zajistit, aby všechna klíčová opatření a politiky byla pravidelně přezkoumávána z hlediska účinnosti a souladu.

3.2 Udržovat auditní stopu a záznamy o nápravných opatřeních za účelem doložení odpovědnosti a zlepšování.

3.3 Připravit organizaci na certifikaci, recertifikaci a programy ujištění zákazníků (např. ISO 27001, onboarding dodavatele).

3.4 Včas identifikovat mezery v kontrolách, aby bylo možné provést rychlou nápravu dříve, než dojde k eskalaci problémů nebo porušení povinností.

3.5 Umožnit generálnímu řediteli a poskytovateli IT podpory koordinovat přezkumy s minimální složitostí při současném zajištění obhajitelných výstupů.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 odpovídá za dohled nad programem auditů,

4.1.2 schvaluje plány interních přezkumů a zjištění,

4.1.3 přiděluje nápravná opatření a sleduje jejich plnění,

4.1.4 schvaluje zapojení externích auditorů nebo konzultantů.

4.2 externí poskytovatel IT služeb / správce

4.2.1 poskytuje důkazy během interních i externích auditů (např. logy, konfigurace, záznamy o řízení přístupu),

4.2.2 podporuje technické kontroly (např. stav zálohování, stav souladu v oblasti patch managementu),

4.2.3 spravuje auditní úložiště důkazů.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Roční přezkum politiky a plánu auditů

9.1.1 generální ředitel (GM) musí tuto politiku a harmonogram auditů přezkoumat nejméně jednou ročně.

9.1.2 Přezkum musí vyhodnotit:

9.1.2.1 účinnost auditů při identifikaci mezer,

9.1.2.2 míru dokončení auditů a nápravných opatření,

9.1.2.3 změny příslušných právních, regulačních nebo certifikačních požadavků.

9.2 Aktualizace na základě spouštěcích událostí

9.2.1 Politika musí být přezkoumána a aktualizována, pokud:

9.2.2 certifikační audit nebo dozorový audit povede k významné neshodě,

9.2.3 dojde ke změně právních nebo regulačních rámců (např. nové pokyny k GDPR, vnitrostátní implementace směrnice NIS2),

9.2.4 změny v podnikání ovlivní systémy, procesy nebo dodavatele zahrnuté do rozsahu auditu,

9.2.5 kritický incident nebo porušení zabezpečení dat odhalí dříve nezjištěné mezery v kontrolách.

9.3 Dokumentace aktualizací

9.3.1 Všechny změny musí být sledovány v protokolu správy verzí politiky.

9.3.2 Aktualizace musí být distribuovány všem členům týmu zapojeným do auditů.

9.3.3 Součástí aktualizované politiky musí být souhrn změn, aby bylo zajištěno jejich porozumění.

10. Související politiky a vazby

10.1 Tato politika je podporována několika dalšími politikami SME a zároveň je posiluje:

10.1.1 P1S – Politika informační bezpečnosti: stanoví základní očekávání pro všechna opatření a vyžaduje jejich uplatňování prostřednictvím auditů.

10.1.2 P2S – Politika rolí a odpovědností v oblasti správy a řízení: stanoví odpovědnost za plánování auditů, jejich provádění a vlastnictví nápravných opatření.

10.1.3 P6S – Politika řízení rizik: identifikuje slabiny bezpečnostních opatření odhalené v auditech a zajišťuje, že zjištění jsou dokumentována v registru rizik.

10.1.4 P17S – Politika ochrany dat a soukromí: vymezuje opatření GDPR, která musí být auditována, včetně nakládání s daty, reakce na porušení zabezpečení a oznámení o ochraně soukromí.

10.1.5 P22S – Politika protokolování a monitorování: poskytuje auditní logy a forenzní data používaná při přezkumech souladu a kontrolách.

10.1.6 P30S – Politika reakce na incidenty: vyžaduje pravidelný audit záznamů o incidentech a přezkoumání po incidentu za účelem ověření účinnosti reakce.

10.1.7 P31S – Politika shromažďování důkazů a forenzní analýzy: poskytuje postupy pro shromažďování ověřitelných důkazů s řetězcem svěření během auditů.

10.2 Tyto politiky společně vytvářejí uzavřené prostředí kontrol, které umožňuje interní ověřování, externí ujištění a správu a řízení v souladu s normami.

11. Referenční normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Kapitola 9.2 – vyžaduje interní audity pro vyhodnocení výkonnosti ISMS a souladu s požadavky.

11.1.2 Kapitola 10.1 – vyžaduje neustálé zlepšování na základě výsledků auditu a nápravy neshod.

11.2 ISO/IEC 27002:

11.2.1 Opatření 5.35 – vyžaduje plánované interní přezkumy opatření a procesů.

11.2.2 Opatření 5.37 – zdůrazňuje nezávislé přezkumy, zejména u outsourcovaných procesů.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Bezpečnostní hodnocení: vyžaduje audity zavedených opatření za účelem ověření jejich účinnosti.

11.3.2 CA-7 – Průběžné monitorování: zdůrazňuje proaktivní odhalování a přezkum slabin opatření.

11.3.3 AU-6 – Přezkum, analýza a vykazování auditů: vyžaduje pravidelnou analýzu auditních logů a zjištění a jejich řešení.

11.4 GDPR EU:

11.4.1 Články 24 a 32 – vyžadují zavedení a audit technických a organizačních opatření, včetně důkazů o účinnosti opatření a zlepšování v čase.

11.5 Směrnice EU NIS2 (2022/2555):

11.5.1 Články 20–21 – vyžadují proaktivní přezkum opatření, soulad založený na důkazech a auditovatelnost pro základní a významné subjekty.

11.6 COBIT 2019:

11.6.1 MEA01 – monitorovat, vyhodnocovat a posuzovat výkonnost a shodu: vyžaduje pravidelné posuzování výkonnosti procesů a opatření vůči normám a cílům.

11.6.2 MEA03 – zajistit soulad s externími požadavky: zaměřuje se na interní monitorování a připravenost na audity třetích stran a regulační přezkumy.