					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P33					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, 9.3, 10	
ISO/IEC 27002:2022	Opatření 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
GDPR	Články 24, 32, 33	
směrnice NIS2	Článek 21(2)(g), 27	
nařízení DORA	Články 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Účel

1.1 Účelem této politiky je stanovit a upravit program organizace pro monitorování auditu a souladu tak, aby:

1.1.1 ověřoval účinnost bezpečnostních opatření a opatření na ochranu soukromí,

1.1.2 zajišťoval soulad s příslušnými normami, právními rámci a smluvními povinnostmi,

1.1.3 včas identifikoval neshody, neefektivity a rizika nesouladu,

1.1.4 podporoval neustálé zlepšování a připravenost na certifikace, hodnocení a regulační přezkumy.

1.2 Tato politika podporuje integritu a vyspělost systému řízení bezpečnosti informací (ISMS) tím, že zavádí strukturované auditorské a monitorovací postupy založené na rizicích a důkazech.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny interní organizační jednotky, funkce a oddělení,

2.1.2 fyzické prostory, cloudová prostředí, platformy SaaS a outsourcované služby,

2.1.3 informační systémy, aplikace, infrastrukturu a datová aktiva spravovaná v rámci ISMS,

2.1.4 zaměstnance, smluvní pracovníky a poskytovatele služeb třetích stran, na které se vztahují auditorské nebo compliance povinnosti.

2.2 Politika zahrnuje:

2.2.1 interní audit,

2.2.2 externí a certifikační audity,

2.2.3 technické monitorování souladu,

2.2.4 audity dodavatelů a třetích stran,

2.2.5 nápravná a preventivní opatření (CAPA),

2.2.6 metriky, řídicí panely a procesy reportingu.

2.3 Vztahuje se na všechny relevantní rámce, jimž organizace podléhá, mimo jiné ISO/IEC 27001, GDPR, směrnici NIS2, nařízení DORA a SOC 2.

3. Cíle

3.1 Ověřovat přiměřenost a účinnost zavedených opatření, politik a postupů v rámci ISMS a souvisejících prostředí.

3.2 Identifikovat a odstraňovat nedostatky, neshody nebo mezery v souladu dříve, než povedou k incidentům nebo porušením.

3.3 Zajišťovat trvalou připravenost na interní přezkumy správy a řízení, externí audity a nezávislé certifikace.

3.4 Vytvářet obhajitelné důkazy a auditní stopy pro potřeby regulačních šetření, právních řízení nebo požadavků zákazníků či partnerů na doložení souladu.

3.5 Začleňovat výsledky auditů do širšího řízení rizik, bezpečnostních metrik a aktivit neustálého zlepšování v organizaci.

4. Role a odpovědnosti

4.1 vedoucí interního auditu / manažer souladu

4.1.1 Plánuje, sestavuje harmonogram a provádí interní audity podle priority rizik.

4.1.2 Spravuje registr auditů, koordinuje auditorské činnosti a sleduje plnění nápravných opatření.

4.2 ředitel informační bezpečnosti (CISO)

4.2.1 Zajišťuje, aby rozsah auditu pokrýval všechny relevantní prvky ISMS a opatření přílohy A.

4.2.2 Dohlíží na ověřování nápravných a preventivních opatření (CAPA) a začleňuje výsledky auditů do bezpečnostního programu.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumána nejméně jednou ročně manažerem souladu a CISO nebo dříve v reakci na:

9.1.1 změny regulačních, smluvních nebo certifikačních rámců,

9.1.2 významná zjištění z auditů nebo opakovaná selhání opatření,

9.1.3 restrukturalizaci organizace nebo změny systému GRC,

9.1.4 doporučení externího auditora nebo zpětnou vazbu regulátora.

9.2 Proces přezkumu musí posoudit:

9.2.1 metodiku plánování auditů a jejich frekvenci,

9.2.2 změny v rozsahu ISMS nebo infrastruktuře,

9.2.3 aktualizace katalogu opatření nebo registru právních požadavků,

9.2.4 konzistenci a kvalitu auditních důkazů a procesů CAPA.

9.3 Veškeré změny politiky musí být:

9.3.1 dokumentovány v repozitáři se správou verzí,

9.3.2 schváleny vrcholovým vedením,

9.3.3 oznámeny veškerému dotčenému personálu a začleněny do aktualizovaných postupů a programů zvyšování povědomí.

9.4 Ověření po přezkumu musí potvrdit, že aktualizované požadavky jsou promítnuty do registru auditů, nástrojů pro zajištění souladu a interních monitorovacích řídicích panelů.

10. Související politiky a vazby

10.1 Tato politika je v souladu s následujícími souvisejícími organizačními politikami:

10.1.1 P1 – P01 Politika informační bezpečnosti: vymezuje ISMS a stanoví odpovědnost za soulad a neustálé zlepšování.

10.1.2 P5 – Politika řízení změn: zajišťuje auditní dohled nad změnami infrastruktury a konfigurace ovlivňujícími prostředí opatření.

10.1.3 P6 – Politika řízení rizik: začleňuje výsledky auditů do hodnocení podnikových rizik a činností ošetření rizik.

10.1.4 P14 – Politika uchovávání údajů: upravuje uchovávání auditních důkazů, logů a záznamů o souladu.

10.1.5 P18 – Politika kryptografických opatření: podporuje bezpečné ukládání a přenos citlivých auditních dat.

10.1.6 P26 – Bezpečnostní politika dodavatelů a poskytovatelů služeb třetích stran: upravuje práva na audit, dokumentaci zajištění a dohled nad souladem dodavatelů.

10.1.7 P30 – Politika reakce na incidenty (P30): slaďuje audity procesů zvládání incidentů s cíli zajištění ISMS.

10.1.8 P32 – Politika kontinuity činností a obnovy po havárii: vyžaduje ověření testování kontinuity a souladu DRP během auditních cyklů.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s globálními normami a právními požadavky pro auditování a průběžné ověřování souladu.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 9.2 – interní audit: vyžaduje pravidelné audity ISMS založené na rizicích za účelem vyhodnocení účinnosti a souladu.

11.2.2 Kapitola 9.3 – přezkoumání ISMS vedením: výsledky auditů musí být vstupem pro strategický přezkum a zlepšování.

11.2.3 Kapitola 10.1 – neshoda a nápravné opatření: zjištění z auditu musí být řešena prostřednictvím dokumentovaných postupů CAPA.

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

11.3.1 Opatření přílohy A 5.35–5.37: pokrývají nezávislý přezkum, soulad s právními a smluvními požadavky a auditní protokolování.

11.3.2 Poskytují návod k implementaci pro plánování, provádění a zlepšování programů auditu a souladu.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – hodnocení opatření: vyžaduje rutinní přezkum zavedených bezpečnostních opatření.

11.4.2 CA-5 – plán opatření a milníků (POA&M): je v souladu se sledováním a nápravou zjištění z auditu.

11.4.3 CA-7 – průběžné monitorování: podporuje proaktivní automatizovaná hodnocení souladu.

11.5 GDPR (2016/679):

11.5.1 Články 24 a 32: vyžadují důkazy o zavedení a účinnosti bezpečnostních opatření prostřednictvím odpovídajících struktur správy a řízení.

11.5.2 Článek 33: podporuje potřebu ověřených auditních stop při reakci na porušení zabezpečení osobních údajů a při oznamování.

11.6 směrnice NIS2 (2022/2555):

11.6.1 Článek 21(2)(g): vyžaduje auditování politik a postupů jako součást minimálních opatření řízení rizik kybernetické bezpečnosti.

11.6.2 Článek 27: vnitrostátní orgány mohou provádět nebo vyžadovat audity u základních a významných subjektů.

11.7 nařízení DORA (2022/2554):

11.7.1 Článek 10(2)(e): subjekty musí provádět interní a externí audity postupů řízení rizik v oblasti ICT.

11.7.2 Článek 25 – požadavky na audit: ukládá povinnost periodických auditů prováděných interními nebo nezávislými externími auditory s dohledem regulačních orgánů.

11.8 COBIT 2019:

11.8.1 MEA01 – monitorovat, vyhodnocovat a posuzovat výkonnost a soulad: zajišťuje, že účinnost opatření je ověřována a vykazována orgánům správy a řízení.

11.8.2 MEA03 – monitorovat, vyhodnocovat a posuzovat soulad: vyžaduje sladění postupů organizace s právními, smluvními a normativními požadavky.