					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P33S					Dokumentum címe: **Audit- és megfelelőségfelügyeleti szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	9.2 és 10. pont	belső auditok, folyamatos fejlesztés és a nemmegfelelőségek helyesbítése
ISO/IEC 27002:2022	5.35 és 5.37 kontroll	ütemezett belső felülvizsgálatok, független felülvizsgálatok kiszervezett folyamatok esetén
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	biztonsági értékelések, folyamatos megfelelőség-monitorozás, auditok felülvizsgálata, elemzése és jelentése
GDPR	24. és 32. cikk	technikai és szervezeti intézkedések auditálása, a kontrollok eredményességének bizonyítékai
NIS2 irányelv	21. cikk (2) bekezdés f) pont	proaktív felülvizsgálat és bizonyítékokon alapuló megfelelés
DORA-rendelet	10. cikk	IKT-kockázatkezelés, monitorozás és jelentéstétel
COBIT 2019	MEA01, MEA03	monitorozás, megfelelőségértékelés, megfelelés, harmadik fél által végzett felülvizsgálatokra való felkészültség

1. Cél

1.1 Jelen szabályzat meghatározza a szervezet belső auditok, biztonsági kontrollok ellenőrzése és a jogszabályi megfelelés nyomon követése tekintetében alkalmazott megközelítését. Biztosítja, hogy valamennyi kontroll, szabályzat, rendszer és szolgáltató rendszeres és strukturált felülvizsgálat alá tartozzon.

1.2 A cél a kontrollhibák feltárása, a nemmegfelelőség megelőzése, valamint az ISO/IEC 27001, a GDPR és a kapcsolódó keretrendszerek szerinti kellő gondosság igazolása.

1.3 A szabályzat lehetővé teszi a KKV-k számára az operatív kontroll fenntartását és a tanúsításra való felkészültség biztosítását dedikált megfelelőségi szervezeti egység nélkül is, egyszerű, ismételhető ellenőrzőlisták és kockázatalapon priorizált megállapítások alkalmazásával.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi belső szervezeti egységre és külső szolgáltatóra, amelyek felelősséggel rendelkeznek az IT-rendszerek, a személyes adatok és az üzletmenet szempontjából kritikus szolgáltatások tekintetében;

2.1.2 az információbiztonság-irányítási rendszer (ISMS) hatálya alá tartozó valamennyi kontrollra és rendszerre;

2.1.3 valamennyi belső audit, biztonsági kontrollfelülvizsgálat és megfelelőségi ellenőrzésre, függetlenül attól, hogy azokat belső erőforrás, külső tanácsadó, ügyfél vagy szabályozó hatóság végzi.

2.2 Jelen szabályzat az alábbiakhoz kapcsolódó bizonyítékgyűjtésre és jelentéstételre is kiterjed:

2.2.1 ISO/IEC 27001 tanúsítási és újratanúsítási auditok;

2.2.2 GDPR vagy szerződéses feltételek szerinti adatvédelmi auditok;

2.2.3 ügyfél által kezdeményezett biztonsági kérdőívek vagy kellő gondossági felülvizsgálatok;

2.2.4 a NIS2 vagy a DORA alapján végzett bármely szabályozói vagy független felülvizsgálat, amennyiben alkalmazandó.

3. Célkitűzések

3.1 Biztosítani kell, hogy valamennyi kulcsfontosságú kontroll és szabályzat eredményességi és megfelelőségi szempontból rendszeres felülvizsgálat tárgyát képezze.

3.2 Fenn kell tartani az auditnyomot és a helyesbítő intézkedések nyilvántartásait az elszámoltathatóság és a fejlesztés igazolása érdekében.

3.3 Biztosítani kell a tanúsítási, újratanúsítási és ügyfélbizonyossági programokra való felkészülést, például az ISO 27001 vagy új beszállítók bevonása esetén.

3.4 A hiányosságokat korai szakaszban azonosítani kell annak érdekében, hogy a helyesbítő intézkedések még azelőtt megtörténjenek, hogy a problémák eszkalálódnának vagy kötelezettségszegéshez vezetnének.

3.5 Az ügyvezetőt és a külső IT-szolgáltatót fel kell hatalmazni arra, hogy a felülvizsgálatokat minimális működési többletterhelés mellett koordinálják, a megfelelés igazolhatóságát biztosító eredményekkel.

4. Szerepkörök és felelősségek

4.1 Ügyvezető

4.1.1 Felügyeli az auditprogramot.

4.1.2 Jóváhagyja a belső felülvizsgálati terveket és a megállapításokat.

4.1.3 Kijelöli és nyomon követi a helyesbítő intézkedéseket.

4.1.4 Engedélyezi külső auditorok vagy tanácsadók bevonását.

4.2 Külső IT-szolgáltató / rendszergazda

4.2.1 Bizonyítékokat biztosít a belső és külső auditok során, például naplókat, konfigurációkat és hozzáférés-kezelési nyilvántartásokat.

4.2.2 Támogatja a műszaki ellenőrzéseket, például a biztonsági mentések állapotának vagy a javításkezelés megfelelőségének vizsgálatát.

4.2.3 Fenntartja az auditbizonyítékok adattárát.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Felülvizsgálati és frissítési követelmények

9.1 A szabályzat és az auditterv éves felülvizsgálata

9.1.1 Az ügyvezető köteles jelen szabályzatot és az auditütemezést legalább évente egyszer felülvizsgálni.

9.1.2 A felülvizsgálat során értékelni kell:

9.1.2.1 az auditok eredményességét a hiányosságok azonosításában;

9.1.2.2 az auditok és a helyesbítő intézkedések teljesítési arányát;

9.1.2.3 az alkalmazandó jogi, szabályozási vagy tanúsítási követelmények változásait.

9.2 Esemény által kiváltott frissítések

9.2.1 A szabályzatot felül kell vizsgálni, és szükség esetén frissíteni kell, ha:

9.2.2 egy tanúsítási vagy felügyeleti audit jelentős nemmegfelelőséget állapít meg;

9.2.3 a jogi vagy szabályozási keretek megváltoznak, például új GDPR-iránymutatás vagy a NIS2 nemzeti átültetése miatt;

9.2.4 üzleti változások érintik az audit hatálya alá tartozó rendszereket, folyamatokat vagy beszállítókat;

9.2.5 egy kritikus incidens vagy adatsértés korábban nem azonosított kontrollhiányosságot tár fel.

9.3 A frissítések dokumentálása

9.3.1 Valamennyi módosítást nyomon kell követni a szabályzati verziónaplóban.

9.3.2 A frissítéseket az auditokban érintett valamennyi munkatárshoz el kell juttatni.

9.3.3 A frissített szabályzathoz mellékelni kell a változások összefoglalását a megfelelő értelmezés biztosítása érdekében.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot több más KKV-szabályzat támogatja és erősíti:

10.1.1 P1S – Információbiztonsági szabályzat: meghatározza valamennyi kontrollal szembeni alapelvárásokat, és előírja ezek auditok útján történő ellenőrzését.

10.1.2 P2S – Irányítási szerepkörök és felelősségek szabályzata: meghatározza az auditok tervezésével, végrehajtásával és a helyesbítő intézkedésekkel kapcsolatos elszámoltathatóságot.

10.1.3 P6S – Kockázatkezelési szabályzat: azonosítja az auditok során feltárt kontrollgyengeségeket, és biztosítja, hogy a megállapítások a kockázati nyilvántartásban rögzítésre kerüljenek.

10.1.4 P17S – Adatvédelmi és a magánszféra védelméről szóló szabályzat: meghatározza az auditálandó GDPR-kontrollokat, beleértve az adatkezelést, az incidenskezelést és az adatvédelmi tájékoztatókat.

10.1.5 P22S – Naplózási és felügyeleti szabályzat: biztosítja a megfelelőségi és kontrollfelülvizsgálatok során használt auditnaplókat és forenzikus adatokat.

10.1.6 P30S – Incidenskezelési szabályzat: előírja az incidensnyilvántartások és az incidens utáni felülvizsgálatok rendszeres auditját a reagálás eredményességének ellenőrzése érdekében.

10.1.7 P31S – Bizonyítékgyűjtési és forenzikai szabályzat: meghatározza az auditok során ellenőrizhető, bizonyítéklánccal alátámasztott bizonyítékok összegyűjtésének eljárásait.

10.2 E szabályzatok együtt zárt kontrollkörnyezetet alkotnak, amely lehetővé teszi a belső ellenőrzést, a külső bizonyosságot és a szabványokkal összhangban álló irányítást.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:

11.1.1 9.2 pont – előírja belső auditok végzését az ISMS teljesítményének és a követelményekkel való összhangjának értékelése érdekében.

11.1.2 10.1 pont – megköveteli a folyamatos fejlesztést az auditok eredményei és a nemmegfelelőségek helyesbítése alapján.

11.2 ISO/IEC 27002:

11.2.1 5.35 kontroll – előírja a kontrollok és folyamatok ütemezett belső felülvizsgálatát.

11.2.2 5.37 kontroll – hangsúlyozza a független felülvizsgálatok fontosságát, különösen kiszervezett folyamatok esetén.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Biztonsági értékelések: előírja a bevezetett kontrollok auditját azok eredményességének ellenőrzése érdekében.

11.3.2 CA-7 – Folyamatos monitorozás: hangsúlyozza a kontrollgyengeségek proaktív feltárását és felülvizsgálatát.

11.3.3 AU-6 – Auditok felülvizsgálata, elemzése és jelentése: előírja az auditnaplók és megállapítások rendszeres elemzését és lezárását.

11.4 GDPR:

11.4.1 24. és 32. cikk – előírja a technikai és szervezeti intézkedések bevezetését és auditálását, beleértve a kontrollok eredményességének és az időbeli fejlesztésnek a bizonyítását.

11.5 NIS2 irányelv (2022/2555):

11.5.1 20–21. cikk – előírja a proaktív kontrollfelülvizsgálatot, a bizonyítékokon alapuló megfelelést és az auditálhatóságot az alapvető és fontos szervezetek számára.

11.6 COBIT 2019:

11.6.1 MEA01 – Teljesítmény és megfelelőség monitorozása, értékelése és vizsgálata: előírja a folyamat- és kontrollteljesítmény rendszeres értékelését a szabványokkal és célokkal szemben.

11.6.2 MEA03 – Külső követelményeknek való megfelelés biztosítása: a belső nyomon követésre és a harmadik fél által végzett auditokra, valamint a szabályozói felülvizsgálatokra való felkészültségre összpontosít.