					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P33					Dokumentum címe: **Audit- és megfelelőség-felügyeleti 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**

A vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	9.2, 9.3, 10. pont	
ISO/IEC 27002:2022	5.35–5.37. kontrollok	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
GDPR	24., 32., 33. cikk	
NIS2 irányelv	21. cikk (2) bekezdés g) pont, 27. cikk	
DORA rendelet	10. cikk (2) bekezdés e) pont, 25. cikk	
COBIT 2019	MEA01, MEA03	

1. Cél

1.1 Jelen szabályzat célja a szervezet audit- és megfelelőség-felügyeleti programjának kialakítása és irányítása annak érdekében, hogy:

1.1.1 ellenőrizze a biztonsági és adatvédelmi kontrollok hatékonyságát,

1.1.2 biztosítsa a vonatkozó szabványokkal, jogszabályi keretrendszerekkel és szerződéses kötelezettségekkel való összhangot,

1.1.3 időben feltárja a nemmegfelelőségeket, a működési hiányosságokat és a megfelelőségi kockázatokat,

1.1.4 támogassa a folyamatos fejlesztést, valamint a tanúsításokra, értékelésekre és szabályozói felülvizsgálatokra való felkészültséget.

1.2 Jelen szabályzat az információbiztonság-irányítási rendszer (ISMS) sértetlenségét és érettségét azáltal támogatja, hogy strukturált, kockázatalapú és bizonyítékokon alapuló audit- és felügyeleti gyakorlatokat épít be.

2. Hatály

2.1 Jelen szabályzat kiterjed az alábbiakra:

2.1.1 belső üzleti egységek, funkciók és szervezeti egységek,

2.1.2 fizikai létesítmények, felhőkörnyezetek, SaaS-platformok és kiszervezett szolgáltatások,

2.1.3 az ISMS által szabályozott információs rendszerek, alkalmazások, infrastruktúra és adatvagyon,

2.1.4 audit- vagy megfelelőségi kötelezettséggel rendelkező munkavállalók, vállalkozók és harmadik fél szolgáltatók.

2.2 A szabályzat az alábbiakat fedi le:

2.2.1 belső audit,

2.2.2 külső/tanúsítási audit,

2.2.3 technikai megfelelőség-felügyelet,

2.2.4 beszállítói és harmadik fél auditok,

2.2.5 helyesbítő és megelőző intézkedések (CAPA),

2.2.6 mutatószámok, irányítópultok és jelentéstételi folyamatok.

2.3 A szabályzat a szervezetre irányadó valamennyi releváns keretrendszerre alkalmazandó, ideértve többek között az ISO/IEC 27001 szabványt, a GDPR-t, a NIS2-t, a DORA rendeletet és a SOC 2-t.

3. Célkitűzések

3.1 Az ISMS-en és a kapcsolódó környezeteken belül bevezetett kontrollok, szabályzatok és eljárások megfelelőségének és hatékonyságának igazolása.

3.2 Az esetleges hiányosságok, nemmegfelelőségek vagy megfelelőségi rések azonosítása és helyesbítése, mielőtt azok incidenssé vagy szabályszegéssé eszkalálódnának.

3.3 A belső irányítási felülvizsgálatokra, külső auditokra és független tanúsításokra való folyamatos felkészültség biztosítása.

3.4 Olyan igazolható bizonyítékok és auditnyom létrehozása, amelyek felhasználhatók szabályozó hatósági megkeresések, jogi eljárások vagy ügyféloldali bizonyossági igények esetén.

3.5 Az audit eredményeinek integrálása a szervezet szélesebb körű kockázatkezelési, biztonsági mutatószám- és folyamatos fejlesztési tevékenységeibe.

4. Szerepkörök és felelősségek

4.1 Belső ellenőrzési vezető / megfelelőségi vezető

4.1.1 Kockázati prioritás alapján megtervezi, ütemezi és végrehajtja a belső auditokat.

4.1.2 Vezeti az auditnyilvántartást, koordinálja az audittevékenységeket, és nyomon követi a helyesbítő intézkedéseket.

4.2 Információbiztonsági vezető

4.2.1 Biztosítja, hogy az audit hatálya az ISMS valamennyi releváns elemére és az A. melléklet kontrolljaira kiterjedjen.

4.2.2 Felügyeli a CAPA-intézkedések ellenőrzését, és integrálja az audit eredményeit a biztonsági programba.

[... 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 Jelen szabályzatot a megfelelőségi vezetőnek és az információbiztonsági vezetőnek legalább évente, vagy szükség esetén korábban felül kell vizsgálnia az alábbi esetekben:

9.1.1 a jogszabályi, szerződéses vagy tanúsítási keretrendszerek változása,

9.1.2 jelentős auditmegállapítások vagy ismétlődő kontrollhibák,

9.1.3 szervezeti átalakítás vagy a GRC-rendszer változásai,

9.1.4 külső auditorok ajánlásai vagy szabályozói visszajelzések.

9.2 A felülvizsgálati folyamatnak értékelnie kell:

9.2.1 az audittervezési módszertant és a gyakoriságot,

9.2.2 az ISMS hatályában vagy infrastruktúrájában bekövetkezett változásokat,

9.2.3 a kontrollkatalógus vagy a jogi nyilvántartás frissítéseit,

9.2.4 az auditbizonyítékok és a CAPA-folyamatok következetességét és minőségét.

9.3 Minden szabályzatmódosítást:

9.3.1 dokumentálni kell verziókezelt adattárban,

9.3.2 a felső vezetésnek jóvá kell hagynia,

9.3.3 közölni kell minden érintett munkatárssal, és be kell építeni a frissített eljárásokba és tudatosságnövelő programokba.

9.4 A felülvizsgálatot követő ellenőrzésnek meg kell erősítenie, hogy a frissített követelmények megjelennek az auditnyilvántartásban, a megfelelőségi eszközökben és a belső felügyeleti irányítópultokon.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat összhangban áll az alábbi kapcsolódó szervezeti szabályzatokkal:

10.1.1 P1 – Információbiztonsági szabályzat: meghatározza az ISMS-t, és rögzíti a megfelelésért és a folyamatos fejlesztésért való elszámoltathatóságot.

10.1.2 P5 – Változáskezelési szabályzat: biztosítja az auditok számára az infrastruktúrát és a kontrollkörnyezetet érintő változások átláthatóságát.

10.1.3 P6 – Kockázatkezelési szabályzat: integrálja az audit eredményeit a vállalati kockázatértékelési és kockázatkezelési tevékenységekbe.

10.1.4 P14 – Adatmegőrzési és megsemmisítési szabályzat: szabályozza az auditbizonyítékok, naplók és megfelelőségi nyilvántartások megőrzését.

10.1.5 P18 – Kriptográfiai kontrollok szabályzata: támogatja az érzékeny auditadatok biztonságos tárolását és továbbítását.

10.1.6 P26 – Harmadik fél és beszállítói biztonsági szabályzat: kiterjed az auditálási jogra, a bizonyossági dokumentációra és a beszállítók megfelelőségi felügyeletére.

10.1.7 P30 – Incidenskezelési szabályzat: összehangolja az incidenskezelési folyamatok auditját az ISMS bizonyossági céljaival.

10.1.8 P32 – Üzletmenet-folytonossági és katasztrófa utáni helyreállítási szabályzat: előírja a folytonossági tesztelés és a DRP-megfelelés ellenőrzését az auditciklusok során.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll az auditálásra és a folyamatos megfelelőség-ellenőrzésre vonatkozó nemzetközi szabványokkal és jogi követelményekkel.

11.2 ISO/IEC 27001:

11.2.1 9.2. pont – Belső audit: előírja az ISMS rendszeres, kockázatalapú auditját a hatékonyság és a megfelelőség értékelése érdekében.

11.2.2 9.3. pont – Vezetőségi felülvizsgálat: az audit eredményeit be kell csatornázni a stratégiai felülvizsgálatba és fejlesztésbe.

11.2.3 10.1. pont – Nemmegfelelőség és helyesbítő intézkedés: az auditmegállapításokat dokumentált CAPA-eljárásokkal kell kezelni.

11.3 ISO/IEC 27002:2022 – 5.35–5.37. kontrollok:

11.3.1 Az 5.35–5.37. kontrollok lefedik a független felülvizsgálatot, a jogi/szerződéses követelményeknek való megfelelést és az auditnaplózást.

11.3.2 Végrehajtási iránymutatást adnak az audit- és megfelelőségi programok tervezéséhez, végrehajtásához és fejlesztéséhez.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Kontrollértékelések: előírja a bevezetett biztonsági kontrollok rendszeres felülvizsgálatát.

11.4.2 CA-5 – Intézkedési és mérföldkőterv (POA&M): összhangban áll az auditmegállapítások nyomon követésével és helyesbítésével.

11.4.3 CA-7 – Folyamatos monitorozás: támogatja a proaktív, automatizált megfelelőségi értékeléseket.

11.5 GDPR (2016/679):

11.5.1 24. és 32. cikk: megfelelő irányítási struktúrákon keresztül előírja a biztonsági kontrollok bevezetésének és hatékonyságának igazolását.

11.5.2 33. cikk: alátámasztja a hiteles auditnyom szükségességét incidenskezelés és bejelentés során.

11.6 NIS2 irányelv (2022/2555):

11.6.1 21. cikk (2) bekezdés g) pont: előírja a szabályzatok és eljárások auditját mint a minimális kiberbiztonsági kockázatkezelési intézkedések részét.

11.6.2 27. cikk: a nemzeti hatóságok auditokat végezhetnek vagy írhatnak elő az alapvető és fontos szervezetek számára.

11.7 DORA rendelet (2022/2554):

11.7.1 10. cikk (2) bekezdés e) pont: előírja az IKT-kockázatkezelési gyakorlatok belső és külső auditját.

11.7.2 25. cikk – Auditkövetelmények: előírja a rendszeres auditokat belső vagy független külső auditorok által, szabályozói átláthatóság mellett.

11.8 COBIT 2019:

11.8.1 MEA01 – Teljesítmény és megfelelőség monitorozása, értékelése és felmérése: biztosítja, hogy a kontrollok hatékonyságát ellenőrizzék és jelentsék az irányító testületek felé.

11.8.2 MEA03 – Megfelelés monitorozása, értékelése és felmérése: előírja a szervezeti gyakorlatok jogi, szerződéses és szabványalapú követelményekkel való összhangját.