					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P05S					Dokumentum címe: **Változáskezelési 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	6.1., 8. pont	
ISO/IEC 27002:2022	8. kontroll	
NIST SP 800-53 Rev.5	CM-2–CM-5, CM-11	
EU NIS2	21. cikk (2) bekezdés b) pont	
EU DORA	6. cikk (9) bekezdés, 8. cikk (4) bekezdés b) pont	
COBIT 2019	BAI06, DSS	

1. Cél

1.1 Jelen szabályzat biztosítja, hogy az informatikai rendszereket, konfigurációkat, üzleti alkalmazásokat vagy felhőszolgáltatásokat érintő valamennyi változás bevezetése előtt megtervezésre, kockázatértékelésre, tesztelésre és jóváhagyásra kerüljön.

1.2 A szabályzat célja az üzemeltetési zavarok, a biztonsági kockázatok és a szolgáltatáskimaradások csökkentése olyan egyszerűsített, ugyanakkor betartható eljárásrend kialakításával, amely korlátozott erőforrásokkal működő kisvállalkozások esetében is alkalmazható.

1.3 Jelen szabályzat az ISO/IEC 27001:2022 szerinti tanúsítás támogatását szolgálja azáltal, hogy formalizálja a műszaki és működési változások kezelésének és dokumentálásának rendjét.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 a változásokat kezdeményező vagy végrehajtó munkavállalókra és részlegvezetőkre,

2.1.2 a rendszereket vagy szoftvereket kezelő külső informatikai szolgáltatókra,

2.1.3 az ügyvezetőre, aki a változások jóváhagyásáért átfogó felelősséget visel.

2.2 A szabályzat az alábbi változásokra terjed ki:

2.2.1 szoftverekre (frissítések, javítócsomagok, új alkalmazások),

2.2.2 hardverekre (cserék, bővítések),

2.2.3 hálózati és tűzfalbeállításokra,

2.2.4 felhőszolgáltatásokra, felhasználói hozzáférési jogosultságokra vagy beszállítói integrációkra,

2.2.5 információs rendszereket és kritikus üzleti folyamatokat érintő változásokra.

2.3 Jelen szabályzat hatálya a tervezett és a rendkívüli változásokra egyaránt kiterjed.

3. Célkitűzések

3.1 Biztosítani kell, hogy minden informatikai és üzleti rendszert érintő változás jóváhagyott, dokumentált és probléma esetén visszaállítható legyen.

3.2 Meg kell előzni a nem szabályozott változásokból eredő, nem tervezett leállásokat, adatvesztést és biztonsági eseményeket.

3.3 Egyszerű, ismételhető eljárásokat kell meghatározni a változások kezdeményezésére, jóváhagyására, tesztelésére és visszaállítására.

3.4 Fenn kell tartani egy auditálható változásnaplót, amely támogatja az üzemeltetési elszámoltathatóságot és a szabályozói megfelelést.

3.5 Lehetővé kell tenni a jelentős vagy érzékeny változások kockázatalapú értékelését és az ezen alapuló döntéshozatalt.

4. Szerepkörök és felelősségek

4.1 Ügyvezető

4.1.1 Végső felelősséget visel minden jelentős változásért.

4.1.2 Felülvizsgálja és jóváhagyja a nem rutinszerű, kritikus vagy magas kockázatú változásokat.

4.1.3 Negyedévente, valamint jelentős incidenseket követően felülvizsgálja a változásnaplót.

4.2 Informatikai támogatás vagy kiszervezett informatikai szolgáltató

4.2.1 Végrehajtja a változásokat, ideértve a konfigurációfrissítéseket, a javítócsomagok telepítését és a rendszeráttelepítéseket.

4.2.2 Fenntart egy alapvető változásnaplót, amely rögzíti a dátumokat, a változások típusát, az eredményeket és a jóváhagyókat.

4.2.3 A bevezetés előtt teszteli a változásokat, és szükség esetén végrehajtja a visszaállítási lépéseket.

4.2.4 A jelentősebb változásokról azok végrehajtása előtt és után tájékoztatja az érintett felhasználókat.

[... 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 Éves felülvizsgálat

9.1.1 Jelen szabályzatot az ügyvezetőnek vagy a kijelölt informatikai kapcsolattartónak évente felül kell vizsgálnia annak biztosítása érdekében, hogy az összhangban maradjon az aktuális rendszerekkel, munkafolyamatokkal és szabályozói követelményekkel.

9.2 Soron kívüli felülvizsgálatok

9.2.1 Felülvizsgálatot kell kezdeményezni az alábbi esetekben is:

9.2.1.1 nem megfelelő változáskezelés által okozott biztonsági incidensek,

9.2.1.2 új informatikai rendszerek bevezetése,

9.2.1.3 a vonatkozó szabványok, például az ISO, a NIS2 vagy a DORA változása.

9.3 A módosítások dokumentálása

9.3.1 Jelen szabályzat módosításait verziókövetetten kell kezelni, és azokat az ügyvezetőnek jóvá kell hagynia. Minden verzióban rögzíteni kell a dátumot, a módosítások összefoglalását és a jóváhagyót.

9.4 A szabályzat kommunikációja

9.4.1 Minden módosításról tájékoztatni kell az összes érintett munkavállalót és külső szolgáltatót. A dokumentációt minden hivatkozott helyen frissíteni kell (pl. munkatársi portálon, megosztott meghajtókon).

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat szorosan kapcsolódik az alábbi SME-szabályzatokhoz:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzat: meghatározza a változások jóváhagyási hatáskörét.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: biztosítja, hogy a változásokból eredő hozzáférés-módosítások megfelelően dokumentálásra és végrehajtásra kerüljenek.

10.1.3 P7S – Beléptetési és kiléptetési szabályzat: összehangolja a szerepkörváltásokhoz és a hozzáférések biztosításához kapcsolódó változásokat.

10.1.4 P15S – Biztonsági mentési és visszaállítási szabályzat: biztosítja, hogy sikertelen változás esetén a visszaállítási és helyreállítási lépések végrehajthatók legyenek.

10.1.5 P30S – Incidenskezelési szabályzat: szabályozza, hogy a sikertelen vagy jogosulatlan változásokat miként kell biztonsági incidensként kezelni.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 6.1. pont – A kockázatalapú tervezésnek ki kell terjednie a változtatási tevékenységekre.

11.1.2 8.1. pont – A működési kontrollokat következetesen alkalmazni kell a változásokhoz kapcsolódó tevékenységeknél a szolgáltatás integritásának biztosítása érdekében.

11.2 ISO/IEC 27002

11.2.1 8.32 kontroll – Iránymutatást ad a biztonságos változáskezelési folyamatokra, beleértve a dokumentálást, a tesztelést és a jóváhagyást.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-2 – A rendszerek előírt alapbeállítása a változtatás előtt.

11.3.2 CM-3 – Konfigurációváltozások szabályozása.

11.3.3 CM-4 – Biztonsági hatáselemzés.

11.3.4 CM-5 – Változások jóváhagyása és dokumentálása.

11.3.5 CM-11 – A változások auditja és nyomon követése.

11.4 EU NIS2 irányelv

11.4.1 21. cikk (2) bekezdés b) pont – Előírja a műszaki és szervezési biztonsági intézkedésekre, ezen belül a változáskezelésre vonatkozó formális eljárásokat.

11.5 EU DORA

11.5.1 6. cikk (9) bekezdés és 8. cikk (4) bekezdés b) pont – Előírja, hogy a pénzügyi szervezetek tartsanak fenn változás- és konfigurációkezelést az IKT-rendszerekre vonatkozóan.

11.6 COBIT 2019

11.6.1 BAI06 – Változások kezelése: kiemeli a tervezést, a kockázatértékelést és a visszaállítási képességet.

11.6.2 DSS01 – Működés irányítása: biztosítja a működési integritást a műszaki átállások és változások során.