					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P05					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**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	6.1. és 5.15. pont	Kiterjed a kockázatkezelési intézkedésekre, a hozzáférés-szabályozásra és a változáskezelésre
ISO/IEC 27002:2022	8.32. kontroll	Strukturált változáskezelési folyamat megvalósítása
NIST SP 800-53 Rev.5	CM-2–CM-14	Konfigurációkezelési kontrollok
GDPR	32. cikk (1) bekezdés b–d pont, 25. cikk, (78) preambulumbekezdés	A rendszerek és adatok biztonságát biztosító technikai és szervezési intézkedések változtatások során
NIS2 irányelv	21. cikk (2) bekezdés a), b), d), e) pont	Előírja az IKT-változásokhoz kapcsolódó kockázatok kezelését
DORA-rendelet	5., 8., 12. cikk	Szabályozza a működési és IKT-kockázatokat, valamint az incidensjelentést
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Strukturált informatikai változáskezelés, teljesítmény- és megfelelőségfelügyelet, valamint követelménykezelés

1. Cél

1.1. Jelen szabályzat formális keretrendszert határoz meg a szervezet információs rendszereit, infrastruktúráját, alkalmazásait és kapcsolódó folyamatait érintő változtatások kezdeményezésére, értékelésére, jóváhagyására, végrehajtására és felülvizsgálatára.

1.2. Biztosítja, hogy minden változtatás szabályozott és auditálható módon történjen, minimalizálva a működési zavarok, a biztonság sérülése vagy a szabályozói megfelelés hiányának kockázatát.

1.3. Támogatja az ISO/IEC 27001:2022 A. melléklet 8.32. kontrollját azáltal, hogy kötelezővé teszi a biztonságos, dokumentált és a kockázatokhoz igazított változáskezelési gyakorlatot.

1.4. A szabályzat továbbá biztosítja a változtatási döntések nyomon követhetőségét, és elősegíti a működési rezilienciát a tervezett vagy rendkívüli módosítások során.

2. Hatály

2.1. Jelen szabályzat az ISMS hatálya alá tartozó rendszereket, adatokat és környezeteket érintő valamennyi változtatásra alkalmazandó, ideértve az alábbiakat:

2.1.1. IT-infrastruktúra (helyszíni, felhőalapú, hibrid)

2.1.2. Éles, előéles és katasztrófa-helyreállítási környezetek

2.1.3. Üzleti alkalmazások, szolgáltatások, API-k és integrációk

2.1.4. Konfigurációs beállítások, javítások telepítése, szoftverkiadások és rendszermigrációk

2.1.5. Rendkívüli javítások, valamint projektalapú vagy tervezett változtatások

2.2. A szabályzat az alábbiak által kezdeményezett változtatásokra terjed ki:

2.2.1. Belső munkatársak (IT-üzemeltetés, fejlesztők, rendszergazdák)

2.2.2. Külső beszállítók, menedzselt szolgáltatók (MSP-k) és vállalkozók

2.2.3. Projektcsapatok rendszerbevezetés, verziófrissítés vagy szolgáltatás-átadás során

2.3. Jelen szabályzat nem alkalmazandó az alábbiakra:

2.3.1. Ideiglenes teszt- vagy fejlesztői környezetekre, amelyek nem férnek hozzá éles adatokhoz

2.3.2. Személyes felhasználói beállításokra (ezeket az Elfogadható Használat szabályzat rendezi)

2.3.3. A szervezet ellenőrzési körén kívül eső rendszerek módosításaira, kivéve, ha azok integrált eszközöket vagy megfelelőségi kötelezettségeket érintenek

3. Célkitűzések

3.1. Biztosítani kell, hogy minden változtatás végrehajtását megelőzően megtörténjen annak felülvizsgálata, jóváhagyása, tesztelése és dokumentálása.

3.2. Fenn kell tartani a rendszerek rendelkezésre állását, az adatok sértetlenségét és a szolgáltatásfolytonosságot a változtatási tevékenységek során és azt követően.

3.3. Elő kell írni a meghatározott változtatási besorolásokat, visszaállítási terveket és kockázatértékeléseket minden változtatástípus esetében.

3.4. Lehetővé kell tenni az átlátható döntéshozatalt és az eszkalációt strukturált irányítási rend mellett.

3.5. Támogatni kell az auditra való felkészültséget nyomon követhető változtatási nyilvántartásokkal és megvalósítást követő felülvizsgálatokkal.

3.6. Biztosítani kell a feladatkörök elkülönítését, és csökkenteni kell a kritikus rendszerekben végrehajtott jogosulatlan vagy egymással ütköző változtatások kockázatát.

4. Szerepkörök és felelősségek

4.1. Felső vezetés

4.1.1. Jóváhagyja a Változáskezelési szabályzatot, és biztosítja annak összhangját a stratégiai célokkal és a szabályozói kötelezettségekkel.

4.1.2. Jóváhagyja a nagy hatású vagy több szakterületet érintő változtatási programokat az irányítási felügyelet részeként.

4.1.3. Biztosítja a változáskezelési eszközökhöz és a munkatársak képzéséhez szükséges erőforrásokat és költségkeretet.

4.2. Változáskezelési Tanácsadó Testület (CAB)

4.2.1. Felülvizsgálja és jóváhagyja a standard és jelentős változtatásokat, biztosítva a kockázatok, hatások és függőségek megfelelő értékelését.

4.2.2. Ellenőrzi a visszaállítási terveket, a teszteredményeket, az érintettek tájékoztatását és az ütemezést.

4.2.3. Tagjai a rendszergazdai, információbiztonsági, IT-üzemeltetési, üzleti és megfelelőségi területek képviselői.

4.2.4. Alacsony kockázatú vagy rendkívüli változtatások esetén dokumentált feltételek mellett döntési jogkört ruházhat át.

4.3. Változtatást kezdeményező

4.3.1. A változtatást a Változáskezelő Rendszerben (CMS) benyújtott, teljes körűen kitöltött változtatási kérelemmel (CR) kezdeményezi.

4.3.2. Biztosítja, hogy a dokumentáció tartalmazza a célokat, a hatályt, az érintett eszközöket, a javasolt ütemezést, a függőségeket, a teszterveket és a visszaállítás lépéseit.

4.3.3. Együttműködik a műszaki csapatokkal és az érintettekkel a megvalósítási és tesztelési szakaszokban.

4.4. Változáskezelési vezető

4.4.1. Kezeli a CMS-t, és biztosítja, hogy minden változtatás megfelelő besorolást, jóváhagyást, ütemezést és felülvizsgálatot kapjon.

4.4.2. Vezeti a CAB-üléseket és karbantartja a központi változtatási naptárat.

4.4.3. Biztosítja, hogy a megvalósítást követő felülvizsgálatok (PIR-ek) elkészüljenek, és a nyilvántartások auditcélokra megőrzésre kerüljenek.

4.5. IT-üzemeltetés és rendszergazdák

4.5.1. Értékelik, végrehajtják és dokumentálják a változtatások műszaki megvalósítását.

4.5.2. Koordinálják a tesztelést, az ellenőrzést és a visszaállítási terveket.

4.5.3. Nem hagyhatnak jóvá és nem hajthatnak végre önállóan olyan rendszerváltoztatásokat, amelyek felett kizárólagos ellenőrzéssel rendelkeznek, független felülvizsgáló bevonása nélkül; ezzel biztosítani kell a feladatkörök elkülönítését.

4.6. Információbiztonság és kockázatkezelés

4.6.1. A CAB jóváhagyását megelőzően értékeli a változtatások biztonsági és megfelelőségi kockázatait.

4.6.2. A változtatás jóváhagyásának előfeltételeként biztonsági vizsgálatot írhat elő (például kódellenőrzést, sérülékenységvizsgálatot, hozzáférés-ellenőrzést).

4.6.3. A változtatást követően felülvizsgálja az új sérülékenységekre vagy váratlan működésre utaló eseményeket.

4.7. Audit és megfelelőség

4.7.1. Felülvizsgálja a változáskezelési folyamat teljességét és eredményességét.

4.7.2. Mintavétellel ellenőrzi a változtatási nyilvántartásokat auditnyom, jóváhagyások, tesztelési bizonyítékok és visszaállítási ellenőrzés szempontjából.

4.7.3. Azonosítja a rendszeres helyesbítést igénylő rendszerszintű kontrollhibákat vagy ismétlődő kivételeket.

5. Irányítási követelmények

5.1. Változtatások besorolása

5.1.1. Minden változtatást kockázat, sürgősség és üzleti hatás alapján kell besorolni:

5.1.1.1. Standard változtatás – Előzetesen jóváhagyott, alacsony kockázatú, gyakran ismétlődő, előre meghatározott eljárásokkal

5.1.1.2. Normál változtatás – Jóváhagyás előtt CAB-felülvizsgálatot és tesztelést igényel

5.1.1.3. Rendkívüli változtatás – Gyorsított felülvizsgálatot igényel; a szokásos CAB-eljárás megkerülhető, de utólagos felülvizsgálatot és PIR-t kell lefolytatni

5.1.1.4. Jogosulatlan vagy nem ütemezett változtatások – Tiltottak, és fegyelmi intézkedést vonnak maguk után

5.1.2. A besorolást a CMS-ben rögzíteni kell, és annak láthatónak kell lennie a központi változtatási naptárban.

5.2. Változtatási kérelmek benyújtása

5.2.1. Minden változtatási kérelemnek tartalmaznia kell:

5.2.1.1. A változtatás leírását, célját és típusát

5.2.1.2. Az érintett rendszereket és függőségeket

5.2.1.3. A változtatás felelősét és a végrehajtó csapatot

5.2.1.4. A tervezett teszteseteket, eredményeket és visszaállítási eljárásokat

5.2.1.5. Az ütemezett végrehajtási időablakot és az érintettek értesítését

5.2.2. A hiányos vagy nem kellően egyértelmű CR-eket a Változáskezelési vezető vagy a CAB elutasítja, illetve javításra visszaküldi.

5.3. Változtatások jóváhagyása és ütemezése

5.3.1. Minden normál és jelentős változtatást a CAB-nak kell jóváhagynia.

5.3.2. A változtatásokat üzletileg kritikus időszakon kívül kell ütemezni, kivéve, ha ettől eltérően indokolt és jóváhagyott döntés születik.

5.3.3. Az ütköző vagy átfedő változtatásokat jelölni és össze kell hangolni a működési zavarok megelőzése érdekében.

5.4. Tesztelés és ellenőrzés

5.4.1. Minden nem triviális változtatást a megvalósítást megelőzően fejlesztői, QA- vagy előéles környezetben kell tesztelni.

5.4.2. Az eredményeket csatolni kell a CR-hez, és azokat a Változáskezelési vezetőnek felül kell vizsgálnia.

5.4.3. Rendkívüli változtatások esetén a tesztelés a megvalósítást követően is történhet, de a szükséges ellenőrzést a PIR során dokumentálni kell.

5.5. Visszaállítás-tervezés

5.5.1. Minden változtatáshoz visszaállítási tervet kell készíteni, amely hiba vagy instabilitás esetén végrehajtható.

5.5.2. A visszaállítási tervnek:

5.5.2.1. Tartalmaznia kell a helyreállítási pontokat és a mentések ellenőrzését

5.5.2.2. Meg kell határoznia a visszaállítást kiváltó feltételeket

5.5.2.3. Meg kell neveznie a felelős személyeket és a döntési jogosultságot

5.5.3. A nem ellenőrzött vagy hiányzó visszaállítási terv a változtatás elutasításának alapját képezi.

6. A szabályzat alkalmazásának követelményei

6.1. Változáskezelő Rendszer (CMS)

6.1.1. Minden változtatási kérelmet, felülvizsgálatot, jóváhagyást és kapcsolódó bizonyító anyagot a központi CMS-ben kell rögzíteni.

6.1.2. A CMS-nek biztosítania kell:

6.1.2.1. A szerepköralapú hozzáférést és az auditnyomot

6.1.2.2. Az állapotkövetést (például: benyújtva, jóváhagyva, végrehajtva, lezárva)

6.1.2.3. Az integrált naptár- és értesítési munkafolyamatokat

6.1.2.4. A teszteredmények, visszaállítási tervek és PIR-ek dokumentumtárolását

6.1.3. Jogosulatlan vagy kizárólag szóbeli változtatás-jóváhagyás szigorúan tilos.

6.2. Kommunikáció és az érintettek tájékoztatása

6.2.1. A változtatást kezdeményezők kötelesek a jóváhagyott normál változtatásokról az érintetteket a végrehajtás előtt legalább 48 órával értesíteni.

6.2.2. Az értesítésnek tartalmaznia kell:

6.2.2.1. A változtatás típusát és a végrehajtási időablakot

6.2.2.2. Az érintett rendszereket és szolgáltatásokat

6.2.2.3. A várható leállást vagy teljesítménycsökkenést

6.2.2.4. A végrehajtás alatti kapcsolattartó adatait

6.2.3. Rendkívüli változtatások esetén az értesítés történhet a megvalósítást követően, de azt a CMS-ben dokumentálni kell.

6.3. Feladatkörök elkülönítése és összeférhetetlenségi kontrollok

6.3.1. Egyetlen személy sem hajthatja végre a teljes változtatási folyamatot (kezdeményezés, jóváhagyás, végrehajtás) felügyelet nélkül.

6.3.2. A CAB és az audit a felülvizsgálatok során ellenőrzi, hogy:

6.3.2.1. A változtatási kérelmek nem önjóváhagyással kerülnek elfogadásra

6.3.2.2. A kiemelt jogosultsággal járó változtatások szakmai ellenőrzés alá esnek

6.3.2.3. Az összeférhetetlenség (például éles hozzáféréssel rendelkező fejlesztő) elkerülésre kerül, vagy naplózással és felügyelettel mérséklik

6.4. Megvalósítást követő felülvizsgálat (PIR)

6.4.1. Minden normál és rendkívüli változtatás esetében a megvalósítást követő 5 munkanapon belül PIR-t kell lefolytatni.

6.4.2. A PIR keretében értékelni kell:

6.4.2.1. A változtatás eredményességét a kitűzött célhoz viszonyítva

6.4.2.2. Az incidenseket vagy a teljesítményre gyakorolt hatást

6.4.2.3. A levont tanulságokat és a folyamatfejlesztési lehetőségeket

6.4.2.4. A végrehajtás és a terv közötti eltéréseket (például ütemezési eltérés, visszaállítás alkalmazása)

6.4.3. A PIR-eket a CR-nyilvántartáshoz kell csatolni, és azokat a Változáskezelési vezetőnek és a CAB-nak felül kell vizsgálnia.

6.5. Rendkívüli változtatások eljárása

6.5.1. Rendkívüli változtatások gyorsított szóbeli vagy átruházott jóváhagyással is végrehajthatók az arra jogosult szerepkörök részéről.

6.5.2. Ezeket a változtatásokat:

6.5.2.1. A végrehajtást követően haladéktalanul dokumentálni kell a CMS-ben

6.5.2.2. A Változáskezelési vezetőnek 24 órán belül felül kell vizsgálnia

6.5.2.3. Kötelező PIR alá kell vonni

6.5.2.4. Ellenőrizni kell a visszaállítás sikeressége szempontjából, ha a végrehajtás hibaelhárítási helyreállítási körülmények között történt

6.5.3. A rendkívüli változtatási eljárás visszaélésszerű alkalmazása a szabályzat megsértése miatti eljárást von maga után.

6.6. Eszközök és automatizálás integrációja

6.6.1. Amennyiben megvalósítható, a változtatási nyilvántartásokat integrálni kell az alábbiakkal:

6.6.1.1. CI/CD-folyamatokkal az automatizált telepítésekhez

6.6.1.2. Verziókezelő rendszerekkel (például Git)

6.6.1.3. Mentési rendszerekkel a visszaállíthatóság biztosítása érdekében

6.6.2. Az eszközök által végrehajtott változtatásoknak is meg kell felelniük jelen szabályzatnak, és azoknak megfelelő CR-azonosítóhoz nyomon követhetően kapcsolódniuk kell.

7. Kockázatkezelés és kivételek

7.1. Változtatásokhoz kapcsolódó kockázatértékelés

7.1.1. Minden változtatás kockázatát az alábbiak alapján kell értékelni:

7.1.1.1. A bizalmasságra, sértetlenségre és rendelkezésre állásra (CIA) gyakorolt hatás

7.1.1.2. A szolgáltatáskimaradás vagy meghibásodás valószínűsége

7.1.1.3. A visszafordíthatóság és a változtatás összetettsége

7.1.1.4. Jogi, megfelelőségi vagy szabályozói következmények

7.1.2. A magas kockázatú változtatások megkövetelhetik:

7.1.2.1. Biztonsági felülvizsgálat lefolytatását

7.1.2.2. További tesztelési ciklusokat

7.1.2.3. Kiterjesztett jóváhagyási munkafolyamatokat

7.1.2.4. A megfelelőségi funkció vagy a szabályozó hatóságok értesítését, ha azt jogszabály előírja

7.2. Kockázatcsökkentő kontrollok

7.2.1. A kockázatcsökkentési intézkedések magukban foglalhatják:

7.2.1.1. Végrehajtás alacsony terhelésű időszakban

7.2.1.2. Párhuzamos telepítéseket vagy blue-green bevezetést

7.2.1.3. Ideiglenes hozzáférés-korlátozások vagy karbantartási mód alkalmazását

7.2.1.4. Mentések és helyreállítás ellenőrzését a változtatás végrehajtása előtt

7.3. Kivételek a változtatási eljárások alól

7.3.1. Jelen szabályzat alóli kivétel kizárólag az alábbi feltételek együttes teljesülése esetén engedélyezhető:

7.3.2. A CISO és a Változáskezelési vezető írásbeli jóváhagyása

7.3.3. Egyértelmű üzleti indokolás és kompenzáló kontrollok

7.3.4. Korlátozott hatály és előre meghatározott lejárat

7.3.5. Kötelező dokumentálás és negyedéves felülvizsgálat

7.3.6. Az ismétlődő vagy rendszerszintű kivételeket az ISMS Irányító Bizottság elé kell terjeszteni.

7.4. Maradványkockázat elfogadása

7.4.1. Ha a kockázatcsökkentés nem lehetséges, a maradványkockázat az alábbi feltételekkel fogadható el:

7.4.1.1. Az indokolás dokumentálása

7.4.1.2. A kockázattulajdonos és az üzleti szponzor jóváhagyása

7.4.1.3. Bejegyzés az ISMS kockázati nyilvántartásába

7.4.1.4. Újraértékelés legalább évente, vagy jelentős változás esetén

8. Betartatás és megfelelés

8.1. Nyomon követés és felügyelet

8.1.1. A Változáskezelési vezető és az ISMS vezető felügyeli a szabályzatnak való megfelelést az alábbiak szerint:

8.1.1.1. Felülvizsgálja a CMS naplóit a jogosulatlan, hiányos vagy dokumentálatlan változtatások azonosítása érdekében

8.1.1.2. Ellenőrzi, hogy minden előírt változtatási elem (jóváhagyás, tesztelés, visszaállítás, PIR) teljesült-e

8.1.1.3. Havi irányítási felülvizsgálatok során mintavétellel ellenőrzi a változtatási nyilvántartásokat

8.1.2. Az automatizált megfigyelő eszközöket úgy kell beállítani, hogy riasztást adjanak az alábbi esetekben:

8.1.2.1. Folyamaton kívül végrehajtott változtatások

8.1.2.2. Olyan rendszermódosítások, amelyek nem kapcsolódnak jóváhagyott CR-hez

8.1.2.3. Konfigurációs eltérés vagy illetéktelen módosítás jóváhagyott változtatást követően

8.2. Meg nem felelés és szabálysértések

8.2.1. Szabálysértésnek minősül különösen:

8.2.1.1. Jogosulatlan vagy dokumentálatlan változtatás

8.2.1.2. A kockázatértékelési vagy visszaállítási követelmények be nem tartása

8.2.1.3. A jóváhagyási nyilvántartásokkal vagy a CMS-munkafolyamatokkal való manipuláció

8.2.1.4. A rendkívüli változtatási eljárás indokolatlan alkalmazása

8.2.2. A meg nem felelés következményei lehetnek:

8.2.2.1. Hozzáférési jogok vagy rendszerjogosultságok visszavonása

8.2.2.2. Fegyelmi intézkedés a HR-szabályzat szerint

8.2.2.3. Harmadik felekkel kötött szerződések megszüntetése

8.2.2.4. Jogi eljárás, ha a változtatás kárt vagy adatnyilvánosságra kerülést okoz

8.2.3. Minden megerősített szabálysértést rögzíteni kell a Szabályzatsértési nyilvántartásban, és a helyesbítő intézkedések végrehajtásáig nyomon kell követni.

8.3. Harmadik felekre vonatkozó követelmények

8.3.1. A változtatást végző beszállítók és vállalkozók kötelesek megfelelni jelen szabályzatnak, és:

8.3.1.1. Auditálhatónak kell lenniük

8.3.1.2. Kötelesek a CMS használatára vagy a változtatások felülvizsgálatra történő benyújtására

8.3.1.3. Szerződéses kikötések útján elszámoltathatók

8.3.2. A tartós meg nem felelés a hatástól függően szerződésbontást, kötbért vagy jogi eljárást eredményezhet.

8.4. Bejelentővédelem és incidensjelentés

8.4.1. Bármely munkavállaló bejelentheti a gyanús változtatásokat vagy folyamatmegkerüléseket a hivatalos biztonsági vagy etikai bejelentési csatornákon keresztül.

8.4.2. Minden bejelentést megtorlás nélkül ki kell vizsgálni, és a megalapozott ügyeket a CISO vagy az Irányító Bizottság elé kell terjeszteni.

9. Felülvizsgálati és módosítási követelmények

9.1. A felülvizsgálat kiváltó okai és gyakorisága

9.1.1. Jelen szabályzatot évente, vagy az alábbi esetek bármelyikében felül kell vizsgálni:

9.1.1.1. Jelentős IT- vagy infrastrukturális változások

9.1.1.2. Sikertelen vagy jogosulatlan változtatásokhoz kapcsolódó jelentős incidensek

9.1.1.3. Szabályozási változások vagy új, változtatásokhoz kapcsolódó jogi kötelezettségek

9.1.1.4. Új eszközök vagy CMS-platformok bevezetése

9.2. A Változáskezelési szabályzat felülvizsgálatának folyamata

9.2.1. A felülvizsgálati folyamatot a Változáskezelési vezető irányítja együttműködésben az alábbiakkal:

9.2.1.1. IT, információbiztonság és üzemeltetés

9.2.1.2. Belső audit és kockázatkezelés

9.2.1.3. A CAB képviselői

9.2.2. A módosításokat a felső vezetésnek és az ISMS Irányító Bizottságnak felül kell vizsgálnia és jóvá kell hagynia.

9.2.3. Az újra kiadott verziókat a dokumentumnyilvántartásban kell nyomon követni, és azokat szükség szerint ismételt tudomásulvétel mellett közölni kell az érintettekkel.

9.3. Dokumentumkezelés és verziókezelés

9.3.1. Minden verziónak tartalmaznia kell:

9.3.1.1. A szabályzat azonosítóját, címét és besorolási szintjét

9.3.1.2. A tulajdonost és a módosítási előzményeket

9.3.1.3. A változásnaplót és a hatálybalépés dátumát

9.3.1.4. A jóváhagyó jogosultságot

9.3.2. Az archivált verziókat a Dokumentummegőrzési szabályzatnak megfelelően kell megőrizni (legalább 3 évig).

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat közvetlenül kapcsolódik az alábbi szabályzatokhoz, és támogatja azok alkalmazását:

10.1.1. P1 – Információbiztonsági szabályzat: Meghatározza a formális biztonsági kontrollok és a folyamatszintű elszámoltathatóság követelményét, beleértve a változáskezelés irányítását.

10.1.2. P2 – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza a változtatások engedélyezéséhez és felügyeletéhez kapcsolódó jóváhagyási jogosultságokat és a feladatkörök elkülönítését.

10.1.3. P4 – Hozzáférés-szabályozási szabályzat: Biztosítja, hogy a változtatásokat végrehajtók és felülvizsgálók hozzáférési jogosultságai a legkisebb jogosultság elvét kövessék.

10.1.4. P6 – Kockázatkezelési szabályzat: Biztosítja, hogy minden változtatás megfelelő kockázatértékelés és kockázatcsökkentő intézkedés alá essen.

10.1.5. P33 – Audit- és megfelelőségfelügyeleti szabályzat: Szabályozza a változáskezelési nyilvántartások és szabálysértések ellenőrzését és auditfelülvizsgálatát.

10.2. E szabályzatok együttesen védhető, nyomon követhető és biztonságos változáskezelési életciklust tesznek lehetővé az ISMS keretrendszerén belül.

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001:2022

11.1.1. 6.1. pont – A kockázatok és lehetőségek kezelésére irányuló intézkedések: Jelen szabályzat támogatja a változtatásokhoz kapcsolódó kockázatok azonosítását, értékelését és kezelését.

11.1.2. 5.15. pont – Hozzáférés-szabályozás: Biztosítja, hogy a változtatások alatti hozzáférések szabályozottak és nyomon követhetők legyenek.

11.1.3. A. melléklet 8.32. kontroll – Változáskezelés: Jelen szabályzat teljes körűen megvalósítja azt a követelményt, hogy az információfeldolgozó létesítmények és rendszerek változtatásait tervezett és szabályozott módon kell kezelni.

11.2. ISO/IEC 27002:2022 – 8.32. kontroll

11.2.1. Megerősíti egy strukturált változáskezelési folyamat alkalmazását, beleértve a változtatások besorolását, jóváhagyását, tesztelését, visszaállítását és dokumentálását.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM kontrollcsalád (CM-1–CM-14): Jelen szabályzat szorosan illeszkedik a konfigurációkezelési kontrollokhoz, beleértve az előírt alapbeállításokat (CM-2), a konfigurációváltozások kontrollját (CM-3), a biztonsági hatáselemzést (CM-4) és a hozzáférési korlátozásokat (CM-5).

11.3.2. AU kontrollcsalád (AU-2, AU-6, AU-12): A jelen szabályzatban hivatkozott naplózási és auditmechanizmusok támogatják a változtatásokhoz kapcsolódó tevékenységek nyomon követhetőségét és a megfelelőség felülvizsgálatát.

11.3.3. RA-3, RA-5: A változtatásvezérelt kockázatértékelések és sérülékenységvizsgálatok a változtatások értékelési folyamatába épülnek be.

11.3.4. PM-11 (Küldetés-/üzleti folyamat meghatározása): Biztosítja, hogy a szolgáltatásfolytonossági és működési célok a változtatások során fennmaradjanak.

11.4. GDPR (2016/679)

11.4.1. 32. cikk (1) bekezdés b–d pont: Jelen szabályzat támogatja a megfelelő technikai és szervezési intézkedések alkalmazásának követelményét az adatbiztonság biztosítása érdekében, különösen rendszerváltoztatások során.

11.4.2. 25. cikk – Beépített és alapértelmezett adatvédelem: Biztosítja, hogy a személyes adatokat érintő változtatások a tervezésbe és a bevezetésbe is beépítsék az adatvédelmi és biztonsági szempontokat.

11.4.3. (78) preambulumbekezdés: Előírja, hogy az adatkezelők olyan mechanizmusokat – például változáskezelési szabályzatokat – alkalmazzanak, amelyek biztosítják a feldolgozási rendszerek folyamatos bizalmasságát, sértetlenségét és ellenálló képességét.

11.5. NIS2 irányelv (2022/2555)

11.5.1. 21. cikk (2) bekezdés a), b), d), e) pont: Előírja az IKT-kockázatok kezelésére szolgáló technikai és szervezési intézkedéseket, beleértve a rendszerváltoztatásokból, szoftverfrissítésekből és infrastrukturális módosításokból eredő kockázatokat is.

11.6. DORA-rendelet (2022/2554)

11.6.1. 5. cikk – Irányítási és belső kontrollkeretrendszer: Jelen szabályzat érvényesíti az IKT-változtatásokhoz és frissítésekhez kapcsolódó működési kockázatkezelési elveket.

11.6.2. 8. cikk – IKT-kockázatkezelési keretrendszer: Előírja, hogy a pénzügyi szervezetek minden, az IKT-rendszereket érintő változtatást strukturált változáskezelési folyamat szerint kezeljenek, amelyet jelen szabályzat a besorolásra, tesztelésre, visszaállításra és dokumentálásra vonatkozó előírásaival tükröz.

11.6.3. 12. cikk – Incidensjelentés: Biztosítja, hogy az IKT-zavarokhoz vezető sikertelen változtatások nyomon követhetők, dokumentáltak és szükség esetén bejelenthetők legyenek.

11.7. COBIT 2019

11.7.1. BAI06 – Menedzselt IT-változtatások: Jelen szabályzat közvetlenül teljesíti a BAI06 célkitűzéseit a változtatások jóváhagyására, hatásértékelésére, kommunikációjára és tesztelésére vonatkozó strukturált munkafolyamatok meghatározásával.

11.7.2. BAI02 – Menedzselt követelménymeghatározás és BAI03 – Menedzselt megoldásazonosítás és fejlesztés: Biztosítja, hogy az üzleti igények által vezérelt változtatások felülvizsgálata és megvalósítása biztonságos módon történjen.

11.7.3. DSS01 – Menedzselt üzemeltetés: Támogatja a rendszerek folyamatos sértetlenségét a változtatások végrehajtása során.

11.7.4. MEA01 és MEA03 – Teljesítmény és megfelelés nyomon követése, értékelése és felmérése: Lehetővé teszi a Változáskezelési szabályzat eredményességének és betartatásának folyamatos felügyeletét.