					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: PII14					Dokumentum címe: **PII biztonsági és hozzáférés-szabályozási 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 / kontroll / cikk	Alkalmazhatóság	Lefedettség típusa	Megjegyzés
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	PII biztonsági kontrollok tervezése és működtetése
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Bizonyítékok, nyomon követés és helyesbítő intézkedés
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identitások és hozzáférési jogosultságok a PII-kezeléshez
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Végpontvédelem és biztonságos hitelesítés
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Naplózás és kriptográfiai védelem
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Alkalmazásbiztonság és biztonságos architektúra
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Nyilvántartások védelme és felülvizsgálata
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Biztonság, elszámoltathatóság és adatfeldolgozói kontrollok
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	ISMS-kontrollok integrációja
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Biztonsági kontrollok bevezetésére vonatkozó iránymutatás
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Információbiztonsági és adatvédelmi megfelelési alapelvek
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4;	Both	Supporting	PII-védelmi biztonsági kontrollok

	Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Hatály

1.1 Ez a szabályzat meghatározza a PII-re vonatkozó biztonsági és hozzáférés-szabályozási követelményeket azon rendszerekre, alkalmazásokra, szolgáltatásokra, eszközökre, felhőkörnyezetekre és működési folyamatokra, amelyek PII-t tárolnak, továbbítanak, kezelnek, elérnek, adminisztrálnak vagy védenek.

1.2 Ez a szabályzat azokra az adatkezelői, közös adatkezelői, adatfeldolgozói és al-adatfeldolgozói környezetekre vonatkozik, amelyekben a szervezet meghatározza, működteti, támogatja vagy igénybe veszi a PII-kezelés biztonsági kontrolljait.

1.3 Ez a szabályzat a következő PII-biztonsági kontrollterületeket fedi le:

1.3.1 PII-biztonsági alapkövetelmények és integráció a meglévő információbiztonsági szabályzatokkal;

1.3.2 hozzáférés-szabályozás;

1.3.3 hitelesítés;

1.3.4 emelt jogosultságú hozzáférés;

1.3.5 titkosítás és biztonságos tárolás;

1.3.6 naplózás és nyomon követés;

1.3.7 biztonságos konfiguráció és sérülékenységkezelés;

1.3.8 végponti és felhő-hozzáférési kontrollok;

1.3.9 bizonyítékok kapcsolása a REG02, REG08, REG10 és REG12 útján.

1.4 Ez a szabályzat nem helyettesíti a teljes információbiztonsági irányítási rendszert, a hálózatbiztonsági szabályzatot, a biztonságos fejlesztési szabályzatot, a biztonsági mentési szabályzatot, a végponti szabályzatot, a felhőbiztonsági szabályzatot, a kriptográfiai szabványt, a sérülékenységkezelési eljárást vagy az incidensreagálási eljárást. Amennyiben ezek a szabályzatok már léteznek, ez a szabályzat meghatározza a PIMS-bizonyossághoz szükséges PII-specifikus kapcsolódási és bizonyítékkövetelményeket.

1.5 Ez a szabályzat nem ismétli meg:

1.5.1 a PII adatkezelési tevékenységek nyilvántartását és a jogalapért való felelősséget a PII03 szerint;

1.5.2 az adatvédelmi kockázat és a DPIA módszertanát a PII07 szerint;

1.5.3 a beépített adatvédelmi kapukat a PII08 szerint;

1.5.4 a gyűjtésre, felhasználásra, külső adatközlésre és adatmegosztásra vonatkozó szabályokat a PII09 szerint;

1.5.5 a megőrzés, törlés és megsemmisítés végrehajtását a PII10 szerint;

1.5.6 az adatfeldolgozói életciklus irányítását a PII12 szerint;

1.5.7 a nemzetközi adattovábbítási mechanizmus kontrolljait a PII13 szerint;

1.5.8 az incidens- és adatsértési munkafolyamatot a PII15 szerint;

1.5.9 a dokumentált információ irányítását a PII17 szerint;

1.5.10 a PIMS nyomon követési, audit- és fejlesztési irányítását a PII18 szerint.

1.6 E szabályzat alkalmazásában az operatív naplók, a biztonsági eszközök kimenetei, a hozzáférési felülvizsgálatok exportjai, a sérülékenységi jelentések és a konfigurációs bizonyítékok olyan bizonyítékforrások, amelyeket a kanonikus bizonyítékobjektumokhoz csatolnak, azokban összefoglalnak vagy azokban hivatkoznak. Ezek nem önálló PIMS-nyilvántartások.

2. Cél

2.1 E szabályzat célja annak biztosítása, hogy a PII a teljes adatkezelés során megfelelő, kockázathoz igazított és auditálható biztonsági és hozzáférési kontrollokkal legyen védve.

2.2 Ez a szabályzat lehetővé teszi a szervezet számára annak igazolását, hogy a PII-biztonsági kontrollokat a REG02, REG08, REG10 és REG12 útján tervezik, vezetik be, vizsgálják felül, követik nyomon és fejlesztik, anélkül, hogy párhuzamos biztonsági nyilvántartásokat hoznának létre vagy helyettesítenék a meglévő információbiztonsági szabályzatokat.

3. Célkitűzések

3.1 E szabályzat célkitűzései a következők:

3.1.1 PII-hozzáférés-szabályozási alapkövetelmény meghatározása rendszerekre és adatkezelési tevékenységekre;

3.1.2 annak biztosítása, hogy a hitelesítési kontrollok megfeleljenek a PII érzékenységének és a hozzáférési környezetnek;

3.1.3 a PII-hez való emelt jogosultságú és normál hozzáférés felülvizsgálati követelményeinek meghatározása;

3.1.4 a tárolt, továbbított, valamint releváns felhő- vagy végponti környezetben lévő PII-re vonatkozó titkosítási és biztonságos tárolási elvárások meghatározása;

3.1.5 a PII-hez való hozzáférés, a PII-t érintő változtatások és a PII adminisztrációja tekintetében a naplózási és nyomon követési elvárások meghatározása;

3.1.6 a PII-t kezelő rendszerekre vonatkozó biztonságos konfigurációs és sérülékenységi bizonyítékkövetelmények meghatározása;

3.1.7 a végponti és felhő-hozzáférési elvárások meghatározása teljes végponti vagy felhőbiztonsági szabályzat létrehozása nélkül;

3.1.8 a feltételezett PII-biztonsági incidensek REG10-hez kapcsolása az incidensmunkafolyamat megkettőzése nélkül;

3.1.9 integráció a meglévő információbiztonsági szabályzatokkal, amennyiben rendelkezésre állnak;

3.1.10 auditra kész bizonyítékok fenntartása kizárólag a REG02, REG08, REG10 és REG12 használatával.

4. Szabályzati rendelkezések

4.1 PII-biztonsági alapkövetelmény és ISMS-integráció

4.1.1 [Both] The Information Security Lead köteles minden PII-t kezelő rendszerre vagy szolgáltatásra vonatkozó PII-biztonsági alapkövetelményt meghatározni a REG12-ben, mielőtt a rendszer vagy szolgáltatás éles üzembe kerül vagy lényegesen megváltozik.

4.1.2 [Both] The System Owner / Application Owner köteles a bevezetett PII-biztonsági kontroll bizonyítékának helyét a REG12-ben rögzíteni, mielőtt meglévő információbiztonsági kontrollra támaszkodik PIMS-bizonyosság céljából.

4.1.3 [Controller] The Process Owner / Business Owner köteles a PII érzékenységét, az adatkezelési környezetet és a hozzáférési igényt a REG02-ben azonosítani, mielőtt új vagy lényegesen módosított PII-hozzáférést kér.

4.1.4 [Processor] The Vendor / Procurement Owner köteles az ügyfél biztonsági utasításait, az ügyfél felelősségi határait és az adatfeldolgozói biztonsági kötelezettségvállalásokat a REG08-ban rögzíteni, mielőtt az adatfeldolgozó hozzáférése az ügyfél PII-jéhez megkezdődik vagy lényegesen megváltozik.

4.1.5 [Both] The Privacy Lead / PIMS Manager köteles ellenőrizni, hogy a PII-biztonsági bizonyíték kapcsolódik-e a REG02, REG08, REG10 vagy REG12 valamelyikéhez, mielőtt az adatkezelési tevékenységet PIMS szempontból auditálhatónak elfogadja.

4.2 Hozzáférés-szabályozási alapkövetelmény

4.2.1 [Both] The System Owner / Application Owner köteles a PII-hez való hozzáférést jóváhagyott szerepkörökre és olyan jogosult felhasználókra korlátozni, akik a REG02-ben vagy REG12-ben rögzítettek vagy visszakövethetők, mielőtt a hozzáférést engedélyezi.

4.2.2 [Both] The Process Owner / Business Owner köteles a PII-hozzáférés üzleti célját a REG02-ben vagy REG12-ben jóváhagyni, mielőtt The System Owner / Application Owner a hozzáférést kiosztja.

4.2.3 [Both] The System Owner / Application Owner köteles legalább negyedévente felülvizsgálni a nagy hatású vagy érzékeny PII-t kezelő rendszerek felhasználói hozzáféréseit, és a felülvizsgálat eredményét a REG12-ben rögzíteni.

4.2.4 [Both] The System Owner / Application Owner köteles legalább évente felülvizsgálni az egyéb PII-t kezelő rendszerek felhasználói hozzáféréseit, és a felülvizsgálat eredményét a REG12-ben rögzíteni.

4.2.5 [Both] The System Owner / Application Owner köteles a PII-hozzáférést szerepkörváltozás, munkaviszony megszűnése, szerződés lezárása vagy a hozzáférési igény megszűnése után egy munkanapon belül a REG12-ben megszüntetni vagy módosítani.

4.2.6 [Processor] The Vendor / Procurement Owner köteles a REG08-ban megerősíteni, hogy az adatfeldolgozói hozzáférés az ügyfél PII-jéhez dokumentált ügyfélutasításokra korlátozódik, mielőtt a hozzáférést engedélyezik vagy módosítják.

4.2.7 [Subprocessor] The Vendor / Procurement Owner köteles a REG08-ban megerősíteni, hogy az al-adatfeldolgozó PII-hozzáférése engedélyezett al-adatfeldolgozói tevékenységekre korlátozódik, mielőtt az al-adatfeldolgozói hozzáférést engedélyezik vagy módosítják.

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

9. Kivételek

9.1.1 [Both] The Information Security Lead köteles minden PII-biztonsági vagy hozzáférés-szabályozási követelmény alóli kivételt a REG12-ben rögzíteni a kivétel aktiválása előtt.

9.1.2 [Both] The Data Protection Officer / Privacy Advisor köteles tanácsot adni a magasabb kockázatú PII-biztonsági kivételekről a REG12-ben a jóváhagyás előtt.

9.1.3 [Both] Top Management köteles a PII-biztonsági kivételeket a REG12-ben jóváhagyni az aktiválás előtt, ha a kivétel nagy hatású PII-t, érzékeny PII-t, emelt jogosultságú hozzáférést, titkosítást, naplózást vagy megoldatlan magas kockázatú sérülékenységeket érint.

9.1.4 [Both] The Information Security Lead köteles a kivétel lejáratát, a kompenzáló kontrollt és a felülvizsgálat dátumát a REG12-ben meghatározni a kivétel jóváhagyása előtt.

9.1.5 [Both] The System Owner / Application Owner köteles a lejárt PII-biztonsági kivételeket a lejáratot követő öt munkanapon belül a REG12-ben helyesbíteni, megújítani vagy lezárni.

9.1.6 [Processor] The Vendor / Procurement Owner köteles az ügyfél PII-jét érintő adatfeldolgozói vagy al-adatfeldolgozói biztonsági kivételeket az elfogadás előtt a REG08-ban és REG12-ben rögzíteni.

10. Betartatás

10.1.1 [Both] The Privacy Lead / PIMS Manager köteles a hiányzó vagy hiányos PII-biztonsági bizonyítékokra vonatkozó meg nem feleléseket az azonosítástól számított öt munkanapon belül a REG12-ben rögzíteni.

10.1.2 [Both] The Information Security Lead köteles a PII-biztonsági kontrollhibák helyesbítésének felelősségét az ellenőrzéstől számított öt munkanapon belül a REG12-ben kijelölni.

10.1.3 [Both] The System Owner / Application Owner köteles a jogosulatlan, túlzott vagy alá nem támasztott PII-hozzáférést az ellenőrzéstől számított egy munkanapon belül letiltani vagy korlátozni, és az intézkedést a REG12-ben rögzíteni.

10.1.4 [Conditional] The Incident Response Coordinator köteles a betartatási intézkedéseket egy munkanapon belül a REG10-hez kapcsolni, ha a betartatási ügy feltételezett vagy megerősített PII-incidenst érint.

10.1.5 [Both] Top Management köteles a visszatérő vagy magas kockázatú PII-biztonsági meg nem feleléseket a REG12-ben felülvizsgálni a vezetőségi felülvizsgálat előtt.

11. Felülvizsgálat és karbantartás

11.1.1 [All] The Privacy Lead / PIMS Manager köteles ezt a szabályzatot The Information Security Lead bevonásával legalább évente felülvizsgálni, és a felülvizsgálat eredményét a REG12-ben rögzíteni.

11.1.2 [Both] The Information Security Lead köteles a PII-biztonsági alapkövetelményt a REG12-ben 30 napon belül felülvizsgálni minden olyan lényeges technológiai, fenyegetési, audit-, incidens- vagy szabályozási változás után, amely a PII-biztonságot érinti.

11.1.3 [Both] The System Owner / Application Owner köteles a rendszerszintű PII-biztonsági bizonyítékokat a REG12-ben 30 napon belül frissíteni minden lényeges architekturális, hozzáférési, konfigurációs, sérülékenységi vagy naplózási változás után.

11.1.4 [Processor] The Vendor / Procurement Owner köteles az adatfeldolgozói és al-adatfeldolgozói PII-biztonsági felelősségi bizonyítékokat a REG08-ban 30 napon belül felülvizsgálni minden lényeges szolgáltatás-, ügyfélutasítás- vagy al-adatfeldolgozói változás után.

11.1.5 [All] The Internal Audit / Compliance Reviewer köteles a jóváhagyott auditterv szerint ellenőrizni a szabályzat felülvizsgálati bizonyítékait és a kiválasztott PII-biztonsági kontrollbizonyítékokat a REG12-ben.

12. Kapcsolódó szabályzatok

12.1 Ezt a szabályzatot a következőkkel együtt kell értelmezni:

12.2 PII01 - Adatvédelmi információirányítási rendszer szabályzat;

12.3 PII02 - Adatvédelmi szerepkörök, felelősségek és elszámoltathatósági szabályzat;

12.4 PII03 - PII adatkezelési tevékenységek nyilvántartása és jogalap szabályzat;

12.5 PII07 - Adatvédelmi kockázatértékelési és DPIA szabályzat;

12.6 PII08 - Beépített és alapértelmezett adatvédelem szabályzat;

12.7 PII09 - PII gyűjtési, felhasználási, külső adatközlési és adatmegosztási szabályzat;

12.8 PII10 - PII megőrzési, törlési és megsemmisítési szabályzat;

12.9 PII12 - Adatfeldolgozói, al-adatfeldolgozói és harmadik fél adatvédelmi irányítási szabályzat;

12.10 PII13 - Nemzetközi PII-továbbítási szabályzat;

12.11 PII15 - PII-incidens- és adatsértés-kezelési szabályzat;

12.12 PII16 - Adatvédelmi képzési, tudatossági és kompetenciaszabályzat;

12.13 PII17 - PIMS dokumentált információ- és bizonyítékkezelési szabályzat;

12.14 PII18 - PIMS nyomon követési, audit- és fejlesztési szabályzat.

13. Hivatkozott szabványok és keretrendszerek

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].