Információbiztonsági Szabályzat (Security Policy)

Dokumentum azonosítója: SURWAYR-SEC-v1.1 **Hatályba lépés dátuma:** 2026. március 28. **Utoljára felülvizsgálva:** 2026. március 28. **Felelős:** CTO / Biztonsági felelős **Vonatkozó szabvány:** ISO/IEC 27001:2022 kontrollok (Annex A hivatkozásokkal)

---

1. Célkitűzés és hatály

Ez a szabályzat a SURWAY'R platform biztonságának irányítási elveit rögzíti az ISO/IEC 27001:2022 szabványban meghatározott kontrollokkal összhangban. A szabályzat minden alkalmazottra, alvállalkozóra és adatfeldolgozóra kiterjed, akik a SURWAY'R rendszereihez hozzáféréssel rendelkeznek.

Keretrendszer hivatkozás: - ISO/IEC 27001:2022 — Annex A kontrollok (A.5–A.8) - GDPR 32. cikk — megfelelő technikai és szervezési intézkedések - ENISA Cloud Security Guidelines

---

2. Szervezési és személyi biztonság (ISO 27001 A.5, A.6)

2.1 Biztonsági felelősségek

- A CTO felelős az információbiztonsági irányítás fenntartásáért.
- Minden alkalmazott és alvállalkozó aláírja a Titoktartási nyilatkozatot (NDA) szerződéskötéskor.
- Érzékeny rendszerekhez (adatbázis, admin panel) csak dokumentált szükségesség alapján kapható hozzáférés.

2.2 Háttér-ellenőrzések

- Rendszerekhez hozzáféréssel rendelkező új munkatársak esetén referencia-ellenőrzés elvégzendő (ISO 27001 A.6.1).
- Alvállalkozók esetén az információbiztonsági követelmények a szerződésben rögzítendők.

2.3 Biztonsági oktatás

- Éves kötelező biztonsági tudatossági képzés minden érintett munkatárs számára (ISO 27001 A.6.3).
- Adathalász-szimulációs tesztek évente legalább egyszer.

---

3. Hozzáférés-kezelés (ISO 27001 A.5.15–A.5.18)

3.1 Szerepköralapú hozzáférés-kezelés (RBAC)

A SURWAY'R a legkisebb jogosultság elvét alkalmazza. Definiált szerepkörök:

Szerepkör	Rendszerek	Jogosultságszint
Admin	Minden rendszer	Teljes
Developer	Alkalmazáskód, staging DB	Olvasás + írás
Support	Felhasználói fiókok (korlátozott)	Olvasás
Olvasó	Analitika, dashboardok	Csak olvasás

3.2 Hozzáférés-jogosultságok felülvizsgálata (Access Review)

- **Negyedéves hozzáférési felülvizsgálat** (ISO 27001 A.5.18): minden felhasználói fiók és jogosultság manuálisan ellenőrzendő.
- Az ex-alkalmazottak és ex-alvállalkozók hozzáféréseit a munkaviszony/megbízás megszűnésének napján visszavonják; legkésőbb 24 órán belül.
- Admin hozzáférésekről negyedévente felülvizsgálati napló készül; ez a DPO és a jogi felelős számára elérhető.

3.3 Kétfaktoros hitelesítés (MFA)

- Az összes admin és fejlesztői fiókhoz kötelező az MFA (TOTP vagy hardveres kulcs) (ISO 27001 A.8.5).
- Kivétel nem megengedett; az MFA-val nem rendelkező fiókok automatikusan letiltásra kerülnek.

3.4 Privilegizált hozzáférések kezelése (Privileged Access Management — PAM)

- Adatbázis és szerver root/admin hozzáférések csak időkorlátozott emelt jogosultsággal érhetők el (just-in-time access).
- Az emelt szintű hozzáférések minden esetben naplózódnak (ki, mikor, mit végzett).
- Személyre szóló root jelszavak nem használhatók; szolgáltatásfiókok és API kulcsok alkalmazandók.

---

4. Kriptográfia és kulcskezelés (ISO 27001 A.8.24)

4.1 Titkosítási előírások

- **Átvitel közben:** TLS 1.2 minimum (TLS 1.3 preferált); SSLv3, TLS 1.0/1.1 tiltott.
- **Tároláskor (alkalmazásszintű érzékeny mezők):** TOTP titkok, AI API kulcsok, webhook aláírási titkok **AES-256-GCM** (AEAD) titkosítással kerülnek tárolásra; **96 bites nonce** CSPRNG-ből; **AAD (additional authenticated data)** kontextus-kötés (`surwayr:v1`). A nonce ütközés valószínűsége elhanyagolható (collision probability negligible). A teljes adatbázis blokk-szintű titkosítása az infrastruktúra (Hetzner) szintjén értelmezett.
- **Jelszavak: Argon2id** (RFC 9106 ajánlott paraméterek: `memory_cost=65536` (64 MiB), `time_cost=3`, `parallelism=4`). A meglévő **bcrypt** hashek továbbra is érvényesek; **sikeres bejelentkezéskor** a rendszer kötelezően **Argon2id-re újra-hasheli** őket (`verify_and_update`). A paraméterek a hardverfejlődéshez igazíthatók (parameters may be adjusted based on hardware evolution).
- **Titkosítási algoritmust** csak a CTO hagyhatja jóvá; gyenge (pl. MD5, SHA-1) algoritmusok tiltottak.
- **Memória és naplók:** Az érzékeny adatokat a rendszer körültekintően kezeli a memóriában; **értékek nem kerülnek alkalmazásnaplókba**.

4.2 Kriptográfiai kulcsok életciklusa (ISO 27001 A.8.24)

Kulcs típusa	Generálás	Tárolás	Rotálás	Lejárati idő
`ENCRYPTION_KEY` (mezőtitkosítás)	CSPRNG (64 hex karakter = 32 bájt)	**Kizárólag** környezeti változó vagy titokkezelő (Vault); **nem**	Évente vagy kompromittálódáskor	Folyamatos

Kulcs típusa	Generálás	Tárolás	Rotálás	Lejárati idő
		tárolható forráskódban vagy verziókezelőben		
API kulcsok (külső)	Biztonságos véletlenszám-generátor (CSPRNG)	Titkosított secrets store (pl. Vault / env)	90 naponta vagy kompromittálódás esetén	1 év max
Adatbázis titkosítási kulcs	KMS (Hetzner / önüzemeltetett)	KMS-ben	Évente	Folyamatos
Felhasználói session tokenek	CSPRNG	HttpOnly, Secure cookie	Session lejártakor	alapértelmezett 24 óra, `SESSION_MAX_AGE` konfigurálható (hitelesített session)
SSL/TLS tanúsítványok	Let’s Encrypt / CA	ACME automatizáció	90 naponta (autorotáció)	90 nap
Backup titkosítási kulcs	CSPRNG	Offline, elkülönített tárolás	Évente	Folyamatos

Kulcs kompromittálódása esetén: azonnali rotálás, incident response folyamat aktiválása, érintett felhasználók értesítése.

---

5. Audit naplózás (ISO 27001 A.8.15)

5.1 Naplózási hatókör

Az alábbi eseményeket kötelező naplózni:

Eseménykategória	Naplózott mezők	Megőrzési idő
Hitelesítés (belépés, kilépés, 2FA)	User ID, IP, időbélyeg, siker/ sikertelenség	12 hónap
Admin műveletek (fiókkezelés, konfiguráció)	Admin ID, tevékenység, érintett erőforrás, időbélyeg	24 hónap
Adatbázis-hozzáférés (SELECT/INSERT/ UPDATE/DELETE)	Query típusa, tábla, user, időbélyeg	12 hónap
API hívások	Endpoint, metódus, user/API key, státuszkód, IP	6 hónap
Exportálási műveletek (SPSS, CSV, JSON)	User ID, survey ID, fájlméret, időbélyeg	12 hónap
Biztonsági incidensek	Minden fenti + kiegészítő kontextus	36 hónap

5.2 Naplók integritása és védelme

- A naplók írás-védett (append-only) tárolóba kerülnek; módosítás nem megengedett.
- A naplók külön szerverre/tárhelyre replikálódnak (a fő alkalmazástól elkülönítve).
- A naplófájlok hash-elt integritás-ellenőrzés alatt állnak (pl. HMAC SHA-256).
- Naplókhoz hozzáférni csak dedikált olvasási jogosultsággal lehet; az alkalmazás írhat, de nem törölhet.

5.3 Naplóriasztások

- Automatizált riasztások az alábbi eseményekre: többszöri sikertelen belépés, admin privilegizált művelet, nagy adatmennyiség exportálása, szokatlan DB-query pattern.

---

6. Fizikai és infrastrukturális biztonság (ISO 27001 A.7)

6.1 Felhőinfrastruktúra

- Az alkalmazás Hetzner Online GmbH szerverein fut (Németország, EU), ISO 27001 tanúsított adatközpontban.
- Fizikai szerverekhez a SURWAY'R munkatársai nem rendelkeznek közvetlen hozzáféréssel.

6.2 Hálózati szegmentáció

- Termelési és fejlesztési/tesztkörnyezetek elkülönítve.
- Adatbázis szerverek nem publikusan elérhetők; csak az alkalmazásszerverről hozzáférhetők VPN/privát hálózaton keresztül.
- Minden bejövő forgalom WAF (Web Application Firewall) mögött.

6.3 Konfigurációkezelés (ISO 27001 A.8.9)

- Az alkalmazásinfrastruktúra **Dockerfile** és **docker-compose** formájában verziókezelt és reprodukálható; minden konfigurációváltozás kódfelülvizsgálaton (PR review) megy keresztül. Dedikált IaC-eszköz (pl. Terraform) bevezetése roadmap elem.
- Alapértelmezett jelszavak és alapértelmezett konfigurációk minden esetben felülírásra kerülnek.

---

7. Sebezhetőség-kezelés (ISO 27001 A.8.8)

7.1 Patch management

- OS és függőségi frissítések: kritikus sebezhetőségek esetén 48 órán belül, egyéb frissítések havi ütemezéssel.
- Automatizált sebezhetőségi szkennelés CI/CD pipeline részeként: **`pip-audit`** (Python függőségek) és **`npm audit`** (JavaScript függőségek) — `main`/`develop` push és heti ütemezés (`.github/workflows/security-audit.yml`). Dependabot / Snyk bevezetése roadmap elem.

7.2 Penetrációs tesztek

- Éves külső penetrációs teszt (minimum évente 1x, célszerűen fehér dobozos módszerrel).
- A tesztjelentések és a megállapítások remediáció-nyilvántartóban kerülnek rögzítésre.

7.3 Sebezhetőség-bejelentési folyamat

A Vulnerability Disclosure Policy (SURWAYR-VDP-v1.0) részletezi, hogyan lehet biztonsági sebezhetőségeket felelősen bejelenteni a security@surwayr.com e-mail-címen.

---

8. Üzletmenet-folytonosság és katasztrófa-helyreállítás (ISO 27001 A.5.29, A.5.30)

Metrika	Célérték	Jelenlegi szint
RTO (Recovery Time Objective)	4 óra	[mérni kell]
RPO (Recovery Point Objective)	1 óra	[mérni kell]
Backup gyakoriság	Naponta (inkrementális) + hetente (teljes)	Konfigurált
Backup tesztelés	Negyedévente teljes visszaállítási teszt	Tervezett
Adatközpont redundancia	Legalább egy géo-replikált backup	Tervezett

---

9. Megfelelőség és auditálhatóság

9.1 Belső audit

- Éves belső auditot kell végezni a jelen szabályzat betartásának ellenőrzésére.
- Az audit megállapításait és a korrekciós intézkedéseket dokumentálva kell tárolni.

9.2 Külső tanúsítványok (roadmap)

Tanúsítvány	Státusz	Tervezett dátum
ISO 27001:2022	Nem tanúsított (irányelvek implementálva)	2026 Q4
SOC 2 Type II	Nem tanúsított	2027

9.3 Adatvédelmi hatásvizsgálat (DPIA — GDPR 35. cikk)

Magas kockázatú adatkezelési tevékenységek bevezetése előtt DPIA elvégzése kötelező, különösen: - Automatizált döntéshozatal bevezetésekor - Különleges adatkategóriák tömeges kezelésekor - Új megfigyelési/profilalkotási funkciók bevezetésekor

---

10. A szabályzat felülvizsgálata

Jelen szabályzatot évente vagy lényeges szervezeti/technológiai változás esetén felül kell vizsgálni. A felülvizsgálatért a CTO felelős, jóváhagyja a vezető.

Kapcsolódó dokumentumok

- Incident Response Plan (SURWAYR-IRP-v1.0)
- Privacy Policy (SURWAYR-PP-v1.1)
- Data Processing Agreement (SURWAYR-DPA-v1.0)
- Vulnerability Disclosure Policy (SURWAYR-VDP-v1.0)
- DSR Policy (SURWAYR-DSR-v1.0)