

# FluxeHRa

ISO Standards Customer Alignment Pack  
ISO/IEC 27001 · 27017 · 27018 · 27701 · 25010

Multi-tenant HRIS — Control alignment & readiness for IT / CISO / DPO / auditors

Generated from application implementation — September 2026 (cover aligned with pack rev. 20)

Companion: [Security & Compliance White Paper](#)

**Not a certification claim.** FluxeHRa is not ISO-certified by virtue of this document. Status values are Implemented / Partial / Platform / Customer / Gap — see §1.

## Available languages / Langues disponibles

English

Français

# ISO Standards Customer Alignment Pack

FluxeHRa / Flex HR — Control alignment & readiness (not a certification claim)

Audience: IT, CISO, DPO, procurement, customer auditors

Document version: September 2026 (rev. 21) — Fluxehra e-signature: eIDAS SES + optional PAdES-B standards

## Table of contents

1. 1. Positioning & how to read this pack
2. 2. ISO/IEC 27001 — Information security management
3. 3. ISO/IEC 27001:2022 Annex A — full control catalogue
4. 4. ISO/IEC 27017 — Cloud services security
5. 5. ISO/IEC 27018 — PII protection in public cloud
6. 6. ISO/IEC 27701 — Privacy information management
7. 7. ISO/IEC 25010 — Software product quality
8. 8. Control matrix (compact thematic view)
9. 9. End-to-end processes catalogue
10. 10. Evidence pack — how to prove it
11. 11. Shared responsibility model (ISO 27017)
12. 12. Recommendations — more auditable & customer-reassuring
13. 13. Known gaps (honest summary)

## 1. Positioning & how to read this pack

**FluxeHRa is not ISO-certified today.** This pack maps product technical controls *and* the full ISO/IEC 27001:2022 Annex A catalogue (including governance, people/HR, and physical dimensions) to help customers see every control area — even those that are organisational rather than code. It is intended for IT due diligence, not as a substitute for a formal ISMS certification audit.

Status legend used throughout:

- **Implemented** — control is implemented in the product and can be demonstrated.
- **Partial** — present but incomplete or limited in coverage.
- **Platform / sub-processor** — primarily delivered by Supabase / Vercel (sub-processors); document in your contracts.
- **Customer responsibility** — remains the customer's (controller's) organizational responsibility.
- **Provider ISMS (Foil Envie)** — Foil Envie SAS organisational ISMS (policies, HR security, premises, supplier program, formal IR drills) — vendor roadmap independent of application features.
- **Gap / roadmap** — known gap; see roadmap (§12).

Companion document: [Security & Compliance White Paper](#) (deeper implementation narrative). Production: <https://fluxehra.ai>.

Internal evidence capture checklist: [docs/iso-evidence-capture-checklist.md](#). Demo session guide: [docs/iso-demo-session-capture-guide.md](#). Gap playbook: [docs/iso-gap-priority-playbook.md](#). Figures under [public/figures/iso-evidence/](#) use real PNG screenshots when available (otherwise SVG placeholders). Nominative Provider evidence stays private (never under [public/](#)).

[↑ Table of contents](#) · [↑ Languages](#)

---

## 2. ISO/IEC 27001 — Information security management

**What it expects:** An Information Security Management System (ISMS): risk-based controls, policies, access management, cryptography, operations, logging, supplier management, people security, physical security, and continual improvement. Annex A (2022) provides a **93-control** catalogue; certification audits the *organization* (here: Foil Envie SAS as processor + the customer as controller), not only software features.

**How FluxeHRa stands:** The SaaS provides strong *technical* Annex A-aligned controls for a multi-tenant HRIS (auth, RBAC, RLS, encryption, audit, hardening). Foil Envie solo-operator ISMS policies (governance, people, home-office physical, suppliers, SDLC) are **signed** (August 2026) and mapped as **Implemented** in §3. Customer controller duties remain with the customer.

**Strengths:** default-deny APIs, RLS tenant isolation, field encryption, MFA, audit trail with proxy accountability, CSP/HSTS/rate limits/SSRF, signed ISMS pack, Axiom SIEM, documented backups.

**Remaining Annex A open items:** customer DPA (A.5.20 / A.5.31); independent ISMS review (A.5.35). A.5.6 closed (Security Watch + signed subscriptions 2026-08-14). **Platform / sub-processor** rows are cloud DC controls, not unfinished product work. Optional: Sentry APM; restore drill after Supabase Pro.

**Customer still should:** maintain their ISMS; perform access reviews; sign DPA; configure MFA enforcement and Turnstile; monitor audit trails; use the AIPD support pack.

[↑ Table of contents](#) · [↑ Languages](#)

---

## 3. ISO/IEC 27001:2022 Annex A — full control catalogue

Full **ISO/IEC 27001:2022 Annex A** catalogue (93 controls). Foil Envie solo-operator ISMS is largely documented and signed (August 2026): most organisational / people / physical rows are **Implemented**. Still open: customer DPA (A.5.20 / A.5.31), independent review (A.5.35). **Platform / sub-processor** rows are cloud data-centre controls (Supabase / Vercel), not product gaps.

### How to read the status and ownership columns

- Implemented** — demonstrable in the FluxeHRa product.
- Partial** — partially covered (product and/or process).
- Platform / sub-processor** — primarily Supabase / Vercel.
- Customer responsibility** — customer (controller) responsibility.
- Provider ISMS (Foil Envie)** — Foil Envie organisational ISMS still open (none today; A.5.6 closed).
- Gap / roadmap** — product / process gap to close.
- App** — fully demonstrable in the FluxeHRa product / CI.
- Company (policy)** — Foil Envie ISMS (HR, legal, physical, external audit).
- Mixed** — product slice + Company (and sometimes Customer) artefacts still required.

### Current status distribution

- Implemented** — **77**

- **Partial** — 3
- **Platform / sub-processor** — 13
- **Customer responsibility** — 0
- **Provider ISMS (Foil Envie)** — 0
- **Gap / roadmap** — 0

#### Ownership distribution (who can close the control)

- **App** — 12
- **Company (policy)** — 40
- **Mixed** — 41

| ID    | Control title                                   | Theme                         | Ownership        | FluxeHRa / Foil Envie note                                                                                                                                                                                                                                                                                                               | Status      |
|-------|-------------------------------------------------|-------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| A.5.1 | Policies for information security               | A.5 — Organizational controls | Company (policy) | Umbrella ISMS governance policy (Certification documentation/policies/ISMS-governance (signed private PDF 2026-08-13)) — Foil Envie solo-operator ISMS Aug 2026.                                                                                                                                                                         | Implemented |
| A.5.2 | Information security roles and responsibilities | A.5 — Organizational controls | Company (policy) | Security & Privacy Owner named (Irwin Rouch) in ISMS-governance (signed private PDF 2026-08-13); product RBAC covers app roles.                                                                                                                                                                                                          | Implemented |
| A.5.3 | Segregation of duties                           | A.5 — Organizational controls | Mixed            | Product: SU vs org admin vs HR; SU tenant access requires Org Admin 48h grant. Solo break-glass signed Aug 2026 (Certification documentation/ops/Break-glass-solo); dual-control planned at hire #2.                                                                                                                                     | Implemented |
| A.5.4 | Management responsibilities                     | A.5 — Organizational controls | Company (policy) | Leadership commitment & resource allocation documented in ISMS-governance (signed private PDF 2026-08-13) (Axiom, MFA, Pro backups, IR, access review).                                                                                                                                                                                  | Implemented |
| A.5.5 | Contact with authorities                        | A.5 — Organizational controls | Company (policy) | CNIL / law-enforcement contact process in ISMS-governance (signed private PDF 2026-08-13) §4; customer remains controller for their notifications.                                                                                                                                                                                       | Implemented |
| A.5.6 | Contact with special interest groups            | A.5 — Organizational controls | Company (policy) | Contact with CERT-FR / CISA / OSV via SU Admin Security Watch (impact-filtered RSS + lockfile) + daily GitHub Action + Dependabot. Signed subscriptions register 2026-08-14 (Certification documentation/policies/Security-community-subscriptions). Email backups: CERT-FR avis, CISA KEV, vendor status. No paid ISAC (proportionate). | Implemented |
| A.5.7 | Threat intelligence                             | A.5 — Organizational controls | Company (policy) | Threat intel: SU Admin Security Watch (OSV/KEV/CERT-FR, impact-filtered) + Dependabot + Components Update + vendor status + Axiom VULN_WATCH (Asset-config-source-privileges signed private PDF 2026-08-13).                                                                                                                             | Implemented |

| ID     | Control title                                             | Theme                         | Ownership        | FluxeHRA / Foil Envie note                                                                                                                                                                                                                 | Status      |
|--------|-----------------------------------------------------------|-------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| A.5.8  | Information security in project management                | A.5 — Organizational controls | Company (policy) | Secure project gates in Secure-development-pack (signed private PDF 2026-08-13) (migrations, typecheck, smoke, secrets, SSRF review).                                                                                                      | Implemented |
| A.5.9  | Inventory of information and other associated assets      | A.5 — Organizational controls | Company (policy) | Foil Envie asset inventory (GitHub, Vercel, Supabase, Axiom, domain, laptop) in Asset-config-source-privileges (signed private PDF 2026-08-13); customers inventory their org data.                                                        | Implemented |
| A.5.10 | Acceptable use of information and other associated assets | A.5 — Organizational controls | Company (policy) | Staff acceptable-use policy (Acceptable-use-remote-clear-desk (signed private PDF 2026-08-13)); product Terms of Use for end users.                                                                                                        | Implemented |
| A.5.11 | Return of assets                                          | A.5 — Organizational controls | Company (policy) | Offboarding & asset return checklist in People-lifecycle (signed private PDF 2026-08-13); product supports org deletion / data return per DPA.                                                                                             | Implemented |
| A.5.12 | Classification of information                             | A.5 — Organizational controls | Mixed            | Product sensitive + visibility; corporate Public/Internal/Confidential/Restricted scheme in Classification-transfer-cloud (signed private PDF 2026-08-13) mapped to ENC2.                                                                  | Implemented |
| A.5.13 | Labelling of information                                  | A.5 — Organizational controls | Company (policy) | Labelling rules for Foil Envie docs/tickets in Classification-transfer-cloud (signed private PDF 2026-08-13) (same scheme as A.5.12).                                                                                                      | Implemented |
| A.5.14 | Information transfer                                      | A.5 — Organizational controls | Mixed            | Product TLS/exports/SSRF; staff email/USB/paper transfer rules in Classification-transfer-cloud (signed private PDF 2026-08-13).                                                                                                           | Implemented |
| A.5.15 | Access control                                            | A.5 — Organizational controls | App              | Product RBAC, RLS, MFA for privileged roles, default-deny APIs; SU org entry gated by customer-approved 48h grant + has_active_su_org_grant RLS.                                                                                           | Implemented |
| A.5.16 | Identity management                                       | A.5 — Organizational controls | App              | Supabase Auth identities; org OIDC SSO; invite / reset flows.                                                                                                                                                                              | Implemented |
| A.5.17 | Authentication information                                | A.5 — Organizational controls | Mixed            | Product password ≥20 + MFA TOTP; staff password-manager + MFA attestation in Staff-auth-secrets (signed private PDF 2026-08-13). Private console: Supabase Auth Multi-Factor TOTP Enabled (ops/Supabase-mfa-totp-enabled-2026-08-16.jpeg). | Implemented |
| A.5.18 | Access rights                                             | A.5 — Organizational controls | Mixed            | Product: Manage Roles, modules; SU temporary org grants with Org Admin accept/deny. Quarterly access-review checklist signed Aug 2026 (Certification                                                                                       | Implemented |

| ID     | Control title                                                     | Theme                         | Ownership        | FluxeHRa / Foil Envie note                                                                                                                                                                                                                                                   | Status      |
|--------|-------------------------------------------------------------------|-------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|        |                                                                   |                               |                  | documentation/ops/Access-review-checklist); re-run each quarter.                                                                                                                                                                                                             |             |
| A.5.19 | Information security in supplier relationships                    | A.5 — Organizational controls | Company (policy) | Private supplier ICT register (Vercel, Supabase, Axiom, Cursor, DocuSign when used) with annual review cadence — Certification documentation/suppliers/Supplier-register.pdf; cert PDFs stay private. Native Fluxehra e-signature is not a separate supplier.                | Implemented |
| A.5.20 | Addressing information security within supplier agreements        | A.5 — Organizational controls | Company (policy) | Sub-processor DPAs / trust docs collected. Customer DPA blocked until first commercial customer (templates + DPA-signature-track signed); other Wave A/B ops docs signed Aug 2026.                                                                                           | Partial     |
| A.5.21 | Managing information security in the ICT supply chain             | A.5 — Organizational controls | Company (policy) | ICT supply-chain covered by Supplier-register (annual calendar + risk notes); ongoing monitoring via vendor status pages and Components Update.                                                                                                                              | Implemented |
| A.5.22 | Monitoring, review and change management of supplier services     | A.5 — Organizational controls | Company (policy) | Supplier-register next-review column + status-page subscriptions documented; annual re-review executed per calendar in private register.                                                                                                                                     | Implemented |
| A.5.23 | Information security for use of cloud services                    | A.5 — Organizational controls | Mixed            | Approved cloud list (Supabase eu-west-1, Vercel dub1, Axiom) + EU preference in Classification-transfer-cloud (signed private PDF 2026-08-13). Private console: Vercel dub1 + Supabase prod FluxeHRa West EU / eu-west-1 (ops/Supabase-prod-general-region-2026-08-16.jpeg). | Implemented |
| A.5.24 | Information security incident management planning and preparation | A.5 — Organizational controls | Mixed            | docs/incident-response.md + solo IR pack signed (Aug 2026): RACI, tabletop 2026-08-11, acknowledgment, Axiom monitors screenshot — private Certification documentation/incident-response/.                                                                                   | Implemented |
| A.5.25 | Assessment and decision on information security events            | A.5 — Organizational controls | Mixed            | Severity matrix in docs/incident-response.md; sole-operator RACI (Irwin Rouch) signed privately (Aug 2026).                                                                                                                                                                  | Implemented |
| A.5.26 | Response to information security incidents                        | A.5 — Organizational controls | Mixed            | Product: bug report / ops / Axiom. Formal IR execution attested via signed solo tabletop + acknowledgment (Aug 2026, private evidence).                                                                                                                                      | Implemented |
| A.5.27 | Learning from information security incidents                      | A.5 — Organizational controls | Mixed            | Post-mortem in IR runbook; signed tabletop gaps/follow-ups on file; annual re-run scheduled; test:security-idor for regressions.                                                                                                                                             | Implemented |

| ID     | Control title                                                          | Theme                         | Ownership        | FluxeHRa / Foil Envie note                                                                                                                                                                                                                                                               | Status                   |
|--------|------------------------------------------------------------------------|-------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| A.5.28 | Collection of evidence                                                 | A.5 — Organizational controls | Mixed            | Product audit logs + compliance export; forensic/evidence playbook in Duty-to-report-and-evidence (signed private PDF 2026-08-13).                                                                                                                                                       | Implemented              |
| A.5.29 | Information security during disruption                                 | A.5 — Organizational controls | Mixed            | Continuity via Supabase/Vercel plans + signed Backup acknowledgment / IR pack (A.5.30). Not a product gap.                                                                                                                                                                               | Platform / sub-processor |
| A.5.30 | ICT readiness for business continuity                                  | A.5 — Organizational controls | Mixed            | Production commitment documented + Backup acknowledgment signed (Aug 2026): Supabase Pro daily backups, 7-day retention, RPO ≤ 24h, internal RTO ≤ 4h (docs/backup-restore.md); Pro + console Backups evidence at first paying customer; restore drill within 30 days of Pro activation. | Implemented              |
| A.5.31 | Legal, statutory, regulatory and contractual requirements              | A.5 — Organizational controls | Mixed            | DPA/legal packs shipped. Blocked on: signed customer DPA + ongoing counsel/legal register reviews (Provider + Customer).                                                                                                                                                                 | Partial                  |
| A.5.32 | Intellectual property rights                                           | A.5 — Organizational controls | Company (policy) | IP / licensing note for Foil Envie code & OSS in Audit-testing-IP-outsourcing (signed private PDF 2026-08-13).                                                                                                                                                                           | Implemented              |
| A.5.33 | Protection of records                                                  | A.5 — Organizational controls | Mixed            | Product retention/purge + corporate records schedule in Records-retention-schedule (signed private PDF 2026-08-13).                                                                                                                                                                      | Implemented              |
| A.5.34 | Privacy and protection of PII                                          | A.5 — Organizational controls | Mixed            | Product privacy: ESS field_consent, My preferences, DSAR, ENC2, PII redact on leak paths; Art.30 processor register docs/registre-activites-traitement-sous-traitant.md. Full PIMS / controller AIPD remains Customer + Provider counsel.                                                | Implemented              |
| A.5.35 | Independent review of information security                             | A.5 — Organizational controls | Company (policy) | Third-party assurance collected for key tooling (e.g. Cursor SOC 2). Blocked on: independent review of FluxeHRa / Foil Envie ISMS (external audit or ISO certification campaign).                                                                                                        | Partial                  |
| A.5.36 | Compliance with policies, rules and standards for information security | A.5 — Organizational controls | Company (policy) | Quarterly compliance self-review defined in ISMS-governance (signed private PDF 2026-08-13) §5 (access review, vuln, suppliers, IR).                                                                                                                                                     | Implemented              |
| A.5.37 | Documented operating procedures                                        | A.5 — Organizational controls | Company (policy) | Ops procedure set: docs/ (IR, backup-restore, SIEM, subprocessors) + signed Certification documentation/ops pack (break-glass, access review, vuln, non-prod, DPA track) and IR/backup acknowledgments.                                                                                  | Implemented              |

| ID    | Control title                                              | Theme                   | Ownership        | FluxeHRa / Foil Envie note                                                                                                                                                                                          | Status                   |
|-------|------------------------------------------------------------|-------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| A.6.1 | Screening                                                  | A.6 — People controls   | Company (policy) | Screening evidence on file + HR security policy signed Aug 2026 (Certification documentation/hr-security/); extend screening to each new hire.                                                                      | Implemented              |
| A.6.2 | Terms and conditions of employment                         | A.6 — People controls   | Company (policy) | Employment confidentiality + NDA + ISMS acknowledgment required (People-lifecycle (signed private PDF 2026-08-13)); NDA signed on file.                                                                             | Implemented              |
| A.6.3 | Information security awareness, education and training     | A.6 — People controls   | Company (policy) | Awareness training completed; HR security policy (signed Aug 2026) mandates annual refresh for staff with system access.                                                                                            | Implemented              |
| A.6.4 | Disciplinary process                                       | A.6 — People controls   | Company (policy) | Disciplinary process for security violations documented in People-lifecycle (signed private PDF 2026-08-13).                                                                                                        | Implemented              |
| A.6.5 | Responsibilities after termination or change of employment | A.6 — People controls   | Company (policy) | Offboarding checklist (revoke GitHub/Vercel/Supabase/Axiom, return assets, NDA reminder) in People-lifecycle (signed private PDF 2026-08-13).                                                                       | Implemented              |
| A.6.6 | Confidentiality or non-disclosure agreements               | A.6 — People controls   | Company (policy) | Partner/tool NDA on file (e.g. Anysphere/Cursor). Employee confidentiality NDA signed for sole operator Irwin Rouch (Aug 2026) — private Certification documentation/hr-security/; reuse template for future hires. | Implemented              |
| A.6.7 | Remote working                                             | A.6 — People controls   | Company (policy) | Remote-work rules (disk encryption, lock screen, no open Wi-Fi for prod admin) in Acceptable-use-remote-clear-desk (signed private PDF 2026-08-13).                                                                 | Implemented              |
| A.6.8 | Information security event reporting                       | A.6 — People controls   | Mixed            | Product in-app bug report + staff duty-to-report procedure in Duty-to-report-and-evidence (signed private PDF 2026-08-13).                                                                                          | Implemented              |
| A.7.1 | Physical security perimeters                               | A.7 — Physical controls | Mixed            | Primary data centres = Supabase/Vercel. Foil Envie home-office perimeter covered under A.7.3 (signed Home-office-physical-media).                                                                                   | Platform / sub-processor |
| A.7.2 | Physical entry                                             | A.7 — Physical controls | Mixed            | Cloud provider physical entry controls. Foil Envie home-office visitor rules under A.7.6 (signed).                                                                                                                  | Platform / sub-processor |
| A.7.3 | Securing offices, rooms and facilities                     | A.7 — Physical controls | Company (policy) | Home-office physical controls (lockable dwelling, no unattended Restricted printouts) in Home-office-physical-media (signed private PDF 2026-08-13).                                                                | Implemented              |
| A.7.4 | Physical security monitoring                               | A.7 — Physical controls | Mixed            | DC CCTV/access logs via cloud providers. Home-office monitoring N/A at DC scale; dwelling lock covered under A.7.3.                                                                                                 | Platform / sub-processor |

| ID     | Control title                                         | Theme                        | Ownership        | FluxeHRA / Foil Envie note                                                                                                                                                                     | Status                   |
|--------|-------------------------------------------------------|------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| A.7.5  | Protecting against physical and environmental threats | A.7 — Physical controls      | Mixed            | Fire/flood/power resilience of cloud regions. Home-office environment covered under Home-office-physical-media (signed).                                                                       | Platform / sub-processor |
| A.7.6  | Working in secure areas                               | A.7 — Physical controls      | Company (policy) | Visitor / secure-work rules for home-office in Home-office-physical-media (signed private PDF 2026-08-13) (no multi-site secure facility).                                                     | Implemented              |
| A.7.7  | Clear desk and clear screen                           | A.7 — Physical controls      | Company (policy) | Clear desk / clear screen in Acceptable-use-remote-clear-desk (signed private PDF 2026-08-13).                                                                                                 | Implemented              |
| A.7.8  | Equipment siting and protection                       | A.7 — Physical controls      | Company (policy) | Equipment siting for operator laptop; cloud hardware = Platform — Home-office-physical-media (signed private PDF 2026-08-13).                                                                  | Implemented              |
| A.7.9  | Security of assets off-premises                       | A.7 — Physical controls      | Company (policy) | Off-premises laptop rules (encryption, minimise local PII) in Home-office-physical-media (signed private PDF 2026-08-13).                                                                      | Implemented              |
| A.7.10 | Storage media                                         | A.7 — Physical controls      | Company (policy) | USB/media handling (prefer cloud; encrypt if used) in Home-office-physical-media (signed private PDF 2026-08-13).                                                                              | Implemented              |
| A.7.11 | Supporting utilities                                  | A.7 — Physical controls      | Mixed            | Power/cooling of cloud DCs. Foil Envie has no dedicated facility utilities (home-office / cloud).                                                                                              | Platform / sub-processor |
| A.7.12 | Cabling security                                      | A.7 — Physical controls      | Mixed            | Cloud DC cabling. Foil Envie has no dedicated comms rooms (home-office / cloud).                                                                                                               | Platform / sub-processor |
| A.7.13 | Equipment maintenance                                 | A.7 — Physical controls      | Mixed            | Cloud hardware maintenance by providers. Operator laptop disposal/wipe under A.7.14 (signed).                                                                                                  | Platform / sub-processor |
| A.7.14 | Secure disposal or re-use of equipment                | A.7 — Physical controls      | Company (policy) | Secure wipe/disposal of Foil Envie devices; cloud destruction = Platform — Home-office-physical-media (signed private PDF 2026-08-13).                                                         | Implemented              |
| A.8.1  | User endpoint devices                                 | A.8 — Technological controls | Company (policy) | Operator endpoint encryption + hardening attestation in Endpoint-malware-attestation (signed private PDF 2026-08-13) (customer devices = Customer).                                            | Implemented              |
| A.8.2  | Privileged access rights                              | A.8 — Technological controls | App              | SU Admin platform isolation; tenant data only with Org Admin—approved 48h grant; MFA aal2 for admin / super_admin / HR / Domain Admin; proxy with audit after enter; service_role server-only. | Implemented              |
| A.8.3  | Information access restriction                        | A.8 — Technological controls | App              | RLS, field visibility, document access routes, org scope asserts.                                                                                                                              | Implemented              |

| ID     | Control title                           | Theme                        | Ownership        | FluxeHRa / Foil Envie note                                                                                                                                                                                                                                                                                              | Status                   |
|--------|-----------------------------------------|------------------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| A.8.4  | Access to source code                   | A.8 — Technological controls | Company (policy) | Private GitHub + least privilege documented in Asset-config-source-privileges (signed private PDF 2026-08-13).                                                                                                                                                                                                          | Implemented              |
| A.8.5  | Secure authentication                   | A.8 — Technological controls | App              | PKCE, password policy ≥20 with mixed case, digit and special character, MFA TOTP for admin / super_admin / HR / Domain Admin (default ON in production), optional Turnstile, org OIDC. Private console: Supabase MFA TOTP Enabled (ops/Supabase-mfa-totp-enabled-2026-08-16.jpeg).                                      | Implemented              |
| A.8.6  | Capacity management                     | A.8 — Technological controls | Mixed            | Elastic capacity via Vercel/Supabase; SU Components Update + Axiom monitors for ops load signals.                                                                                                                                                                                                                       | Platform / sub-processor |
| A.8.7  | Protection against malware              | A.8 — Technological controls | Company (policy) | OS AV/Defender attestation + product SCORM zip limits — Endpoint-malware-attestation (signed private PDF 2026-08-13).                                                                                                                                                                                                   | Implemented              |
| A.8.8  | Management of technical vulnerabilities | A.8 — Technological controls | App              | Components Update + Security Watch (OSV/KEV) + Dependabot PRs + CI `npm run audit:deps` (high/critical) with AUDIT_ALLOWLIST waivers; SLA Critical ≤7d / High ≤30d surfaced in SU Admin.                                                                                                                                | Implemented              |
| A.8.9  | Configuration management                | A.8 — Technological controls | Mixed            | Config baselines (migrations, vercel.json, env inventory) in Asset-config-source-privileges (signed private PDF 2026-08-13).                                                                                                                                                                                            | Implemented              |
| A.8.10 | Information deletion                    | A.8 — Technological controls | App              | Org cascade delete, DSAR anonymize, retention purge APIs.                                                                                                                                                                                                                                                               | Implemented              |
| A.8.11 | Data masking                            | A.8 — Technological controls | App              | At-rest ENC2 encryption + role-scoped decrypt; authorized CSV/API/SFTP/DSAR stay plaintext. Leak channels (bug/error) redact IBAN/SSN-like patterns.                                                                                                                                                                    | Implemented              |
| A.8.12 | Data leakage prevention                 | A.8 — Technological controls | Mixed            | Product DLP baseline: export auth, rate limits, private storage, bug-path PII redact, BULK_EXPORT security events on key exports. Enterprise CASB/endpoint DLP not deployed (Customer/Provider optional).                                                                                                               | Implemented              |
| A.8.13 | Information backup                      | A.8 — Technological controls | Mixed            | Supabase Pro daily backups (7-day retention) committed for first paying customer; RPO ≤ 24h and internal RTO ≤ 4h in docs/backup-restore.md and signed Backup acknowledgment (Aug 2026); optional PITR add-on; Storage objects not in DB backup (documented). Live Backups UI screenshot deferred until Pro activation. | Implemented              |
| A.8.14 | Redundancy of information               | A.8 — Technological controls | Mixed            | Cloud multi-AZ resilience of providers. Foil Envie RPO/RTO documented in backup-                                                                                                                                                                                                                                        | Platform / sub-processor |

| ID     | Control title                                   | Theme                        | Ownership        | FluxeHRa / Foil Envie note                                                                                                                                                                                                                                                             | Status                   |
|--------|-------------------------------------------------|------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|        | processing facilities                           |                              |                  | restore.md (A.5.30). Multi-region active-active not claimed.                                                                                                                                                                                                                           |                          |
| A.8.15 | Logging                                         | A.8 — Technological controls | App              | audit_logs (business trail) + structured SECURITY_EVENT SIEM via Axiom (fluxehra_logs); PII-safe authz/tenant/RLS/auth-failure/cron/HMAC/SSRF telemetry (Aug 2026 rev. 6).                                                                                                             | Implemented              |
| A.8.16 | Monitoring activities                           | A.8 — Technological controls | Mixed            | Axiom monitors (3 slots) live: BOLA/tenant, per-IP brute-force, high-signal (cron/RLS/HMAC/SSRF); private evidence EV-SIEM-AXIOM-monitors.png (Aug 2026); Vercel Analytics + ops events; solo IR RACI for response. Not a 24x7 outsourced SOC.                                         | Implemented              |
| A.8.17 | Clock synchronization                           | A.8 — Technological controls | Mixed            | Cloud NTP via providers; app timestamps from server clocks.                                                                                                                                                                                                                            | Platform / sub-processor |
| A.8.18 | Use of privileged utility programs              | A.8 — Technological controls | Company (policy) | Prod DB/console utilities restricted to Security Owner — Asset-config-source-privileges (signed private PDF 2026-08-13) + Break-glass-solo.                                                                                                                                            | Implemented              |
| A.8.19 | Installation of software on operational systems | A.8 — Technological controls | Mixed            | Production deploys only via Vercel CI from authorised repo — Asset-config-source-privileges (signed private PDF 2026-08-13).                                                                                                                                                           | Implemented              |
| A.8.20 | Networks security                               | A.8 — Technological controls | Mixed            | Cloud network security of providers. Operator remote-work network hygiene under Acceptable-use-remote-clear-desk (signed).                                                                                                                                                             | Platform / sub-processor |
| A.8.21 | Security of network services                    | A.8 — Technological controls | App              | HTTPS/HSTS; SSRF guard on webhooks, SFTP, OIDC token/JWKS, SMTP hosts, and IdP authorize/SAML SSO URLs (https + public hosts only).                                                                                                                                                    | Implemented              |
| A.8.22 | Segregation of networks                         | A.8 — Technological controls | Mixed            | Cloud VPC / isolation. Foil Envie prod vs Dev: separate Vercel projects (fluxehra.ai vs saas-flex-hr-sql-dev) + separate Supabase FluxeHRa-dev (eu-west-1); private console captures under Certification documentation/ops/; non-prod data policy (signed) + assertNonProdSupabaseUrl. | Platform / sub-processor |
| A.8.23 | Web filtering                                   | A.8 — Technological controls | Company (policy) | N/A enterprise web proxy (no device fleet); compensating SmartScreen/Defender + DNS hygiene on operator laptop — Certification documentation/policies/Web-filtering-NA-compensating. Reassess when staff fleet grows.                                                                  | Implemented              |
| A.8.24 | Use of cryptography                             | A.8 — Technological controls | App              | TLS in transit; AES-256-GCM field encryption; encrypted DocuSign private key at rest when that engine is used;                                                                                                                                                                         | Implemented              |

| ID     | Control title                                               | Theme                        | Ownership        | FluxeHRA / Foil Envie note                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Status      |
|--------|-------------------------------------------------------------|------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|        |                                                             |                              |                  | FluxeHRA e-signature tokens/OTP stored hashed only.                                                                                                                                                                                                                                                                                                                                                                                                                                           |             |
| A.8.25 | Secure development life cycle                               | A.8 — Technological controls | Mixed            | Secure SDLC policy in Secure-development-pack (signed private PDF 2026-08-13) (migrations, typecheck, smoke, CSP practices).                                                                                                                                                                                                                                                                                                                                                                  | Implemented |
| A.8.26 | Application security requirements                           | A.8 — Technological controls | Mixed            | Application security requirements checklist in Secure-development-pack (signed private PDF 2026-08-13) (RLS, authz, secrets, SSRF, ENC2).                                                                                                                                                                                                                                                                                                                                                     | Implemented |
| A.8.27 | Secure system architecture and engineering principles       | A.8 — Technological controls | App              | Browser untrusted; server authz; RLS; defence in depth (documented in whitepaper).                                                                                                                                                                                                                                                                                                                                                                                                            | Implemented |
| A.8.28 | Secure coding                                               | A.8 — Technological controls | Mixed            | Secure-coding checklist (escapeHtml/DOMPurify/path gateway/audit:deps) in Secure-development-pack (signed private PDF 2026-08-13).                                                                                                                                                                                                                                                                                                                                                            | Implemented |
| A.8.29 | Security testing in development and acceptance              | A.8 — Technological controls | Mixed            | Acceptance gates: security-smoke, security-idor, audit:deps via GitHub Actions workflow security-tests + Secure-development-pack (signed private PDF 2026-08-13). External pen-test remains future engagement.                                                                                                                                                                                                                                                                                | Implemented |
| A.8.30 | Outsourced development                                      | A.8 — Technological controls | Company (policy) | No outsourced development currently; contractor rules defined if engaged — Audit-testing-IP-outsourcing (signed private PDF 2026-08-13).                                                                                                                                                                                                                                                                                                                                                      | Implemented |
| A.8.31 | Separation of development, test and production environments | A.8 — Technological controls | Mixed            | Dedicated dual tracks (Aug 2026): Git main → Vercel saas-flex-hr-sql + Supabase FluxeHRA (prod, eu-west-1); Git dev → Vercel saas-flex-hr-sql-dev + Supabase FluxeHRA-dev (eu-west-1). Private evidence: ops/EV-ENV-SEPARATION-*-2026-08-16.png plus console captures (prod domains, dub1, env names, Deployment Protection, prod region, Auth URLs) — docs/provider-isms-evidence.md. Non-prod data policy signed; assertNonProdSupabaseUrl when PRODUCTION_SUPABASE_URL set on Preview/Dev. | Implemented |
| A.8.32 | Change management                                           | A.8 — Technological controls | Mixed            | Change management = Git + Vercel deploy for solo operator (Secure-development-pack (signed private PDF 2026-08-13)); CAB deferred until team growth.                                                                                                                                                                                                                                                                                                                                          | Implemented |
| A.8.33 | Test information                                            | A.8 — Technological          | Mixed            | Dummy-data tooling + non-prod data policy signed Aug 2026 (no prod dumps;                                                                                                                                                                                                                                                                                                                                                                                                                     | Implemented |

| ID     | Control title                                          | Theme                        | Ownership        | FluxeHRa / Foil Envie note                                                                                             | Status      |
|--------|--------------------------------------------------------|------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------|-------------|
|        |                                                        | controls                     |                  | redact if copy ever needed) — Certification documentation/ops/Non-prod-data-policy.                                    |             |
| A.8.34 | Protection of information systems during audit testing | A.8 — Technological controls | Company (policy) | Rules for customer/vendor audit testing vs production in Audit-testing-IP-outsourcing (signed private PDF 2026-08-13). | Implemented |

This catalogue is a living SoA-style view for customer due diligence. Remaining **Partial** rows are A.5.20, A.5.31, A.5.35.

**Platform / sub-processor** = sub-processor data-centre controls. **Provider ISMS (Foil Envie)** count is 0.

[↑ Table of contents](#) · [↑ Languages](#)

## 4. ISO/IEC 27017 — Cloud services security

**What it expects:** Cloud-specific guidance extending 27001: shared responsibility, virtualization/admin separation, customer data isolation, cloud logging, and clarity of cloud service customer vs provider duties.

**How FluxeHRa stands:** Explicit shared-responsibility model (§11): customer (controller) → FluxeHRa app controls → Foil Envie ISMS ( **Provider ISMS (Foil Envie)** ) → Supabase/Vercel. Multi-tenant isolation via RLS + API scope; privileged proxy does not elevate JWT/RLS; org admin SSO to customer IdP supported.

**Strengths:** tenant RLS, org-scoped storage paths, per-integration export HMAC/IP allow-list options, documented EU regions, SU data access gated by 48h Org Admin grant (deploy of default config is separate change-management control).

**Residual:** customers should retain sub-processor contracts; Foil Envie documents EU regions and Supabase Pro backup RPO≤24h / internal RTO≤4h. Customer DPA signature remains A.5.20 / A.5.31.

**Customer still should:** configure SSO, roles, session policy; review SU vs org admin privileges; retain cloud contracts and region evidence.

[↑ Table of contents](#) · [↑ Languages](#)

## 5. ISO/IEC 27018 — PII protection in public cloud

**What it expects:** Controls for protecting personally identifiable information (PII) processed by public cloud processors: purpose limitation, transparency, data return/erasure, disclosure, and security of PII.

**How FluxeHRa stands:** HR PII is core to the product. Technical protections include sensitive-field encryption, visibility minimization, private DMS, EU hosting alignment, hashed public tokens for new-hire data collection. The product does not use customer HR data for advertising or unrelated secondary purposes.

**Strengths:** encryption + visibility + private documents + org deletion + DSAR export/anonymize + real retention purge.

**Residual:** special-category ESS consent is persisted via `field_consent`s + My preferences withdraw. No ISO/SOC *certificate* is claimed (external campaign = A.5.35).

**Customer still should:** define lawful basis, retention schedules, DPIA; use in-product DSAR export/anonymize and retention purge; execute signed DPA.

[↑ Table of contents](#) · [↑ Languages](#)

## 6. ISO/IEC 27701 — Privacy information management

**What it expects:** Extension of 27001/27002 for a Privacy Information Management System (PIMS), clarifying controller vs processor obligations and PII processing controls.

**How FluxeHRa stands:** Typically acts as **processor** for customer employee data; customer is **controller**. Product supplies technical PIMS measures (visibility, DSAR, retention purge, consents, Art.30 processor register, IR). Controller DPIA / lawful basis / signed customer DPA remain Customer (A.5.20 / A.5.31).

**Strengths:** field-level access control, encryption, auditability of admin actions, tokenized candidate data request, org-wide deletion, AIPD support pack, DSAR export/anonymize, Trust Center.

**Residual:** signed customer DPA (first commercial customer); independent certification campaign (A.5.35). Core HR write auditing is implemented.

**Customer still should:** appoint DPO as required; execute DPA; instruct retention; run subject-rights procedures.

[↑ Table of contents](#) · [↑ Languages](#)

## 7. ISO/IEC 25010 — Software product quality

**What it expects:** A quality model: functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, portability.

**How FluxeHRa stands:**

- **Functional suitability:** Core HR (bitemporal), performance, learning, compensation, analytics, integrations — recruitment still placeholder.
- **Security:** layered controls described in §§2–6 and whitepaper.
- **Usability:** role-based shells (HR / manager / employee / SU); schema-driven forms.
- **Reliability / maintainability:** migrations, security-tests CI, Components Update SLA; Axiom SIEM. Optional Sentry APM is extra observability, not an Annex A blocker.

**Customer still should:** UAT against their HR processes; monitor availability via status/ops agreements.

[↑ Table of contents](#) · [↑ Languages](#)

## 8. Control matrix (compact thematic view)

High-level themes (see §3 for the full Annex A dump). Evidence IDs link to §10.

| Control theme                    | Expectation                                                              | FluxeHRa implementation                                                                                                                                  | Status      | Evidence ID                 |
|----------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-----------------------------|
| Access control (27001 A.8)       | Authenticate users; enforce least privilege; protect privileged accounts | Supabase Auth (PKCE/JWT), RBAC, HR geo scope, MFA TOTP for admin/super_admin/hr/Domain Admin (default ON in production), idle timeout, default-deny APIs | Implemented | EV-AUTH-MFA, EV-RBAC-ROLES  |
| Cryptography (27001 A.8)         | Protect confidentiality of sensitive data in transit and at rest         | HTTPS/HSTS; AES-256-GCM field encryption ( ENC2:: ) for sensitive schema fields; hashed integration keys                                                 | Implemented | EV-CRYPTO-FIELD             |
| Logging & monitoring (27001 A.8) | Record security-relevant events with accountable identity                | audit_logs with real vs proxied user; Audit Trail UI; Core HR hire/update/terminate audited; export fingerprint for integrations                         | Implemented | EV-AUDIT-TRAIL, EV-PROXY    |
| Secure development               | Apply secure SDLC, dependency hygiene,                                   | TypeScript strict build, migrations, security-tests CI                                                                                                   | Implemented | EV-SDLC-TESTS, EV-SECURITY- |

| Control theme                        | Expectation                                                                  | FluxeHRa implementation                                                                                                                                                     | Status                   | Evidence ID                                                                     |
|--------------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|---------------------------------------------------------------------------------|
| (27001 A.8)                          | change control                                                               | (smoke/IDOR/audit:deps), Components Update + SLA, signed Secure-development-pack, SU Admin Security Watch + Dependabot (A.5.6)                                              |                          | WATCH, EV-ENV-SEPARATION                                                        |
| Network & application hardening      | Reduce attack surface (headers, rate limits, SSRF, XSS)                      | CSP (nonce + strict-dynamic), HSTS, X-Frame-Options, rate limits, SSRF guard, DOMPurify/escapeHtml, Turnstile                                                               | Implemented              | EV-HEADERS-CSP, EV-TURNSTILE                                                    |
| Supplier / cloud (27001 A.5; 27017)  | Manage cloud shared responsibility and sub-processors                        | Documented sub-processors Supabase (eu-west-1) + Vercel (dub1); Security Watch (CERT-FR / CISA / OSV); customer DPA/contracts outside product                               | Platform / sub-processor | EV-HOSTING-REGIONS, EV-SECURITY-WATCH, EV-SUPPLIER-VERCEL, EV-SUPPLIER-SUPABASE |
| Tenant isolation (27017)             | Separate customer environments/data in multi-tenant cloud                    | Shared-schema multi-tenancy with <code>organization_id</code> + PostgreSQL RLS; API <code>assertOrganizationScope</code> ; org-prefixed storage paths                       | Implemented              | EV-RLS-TENANT                                                                   |
| Customer admin capabilities (27017)  | Secure privileged customer administration and virtualization/proxy           | Org Admin / SU Admin roles; SU tenant entry requires Org Admin-approved 48h grant ( <code>su_org_access_grants</code> ); proxy only after enter with dual audit attribution | Implemented              | EV-PROXY, EV-SU-ORG-ACCESS, EV-RBAC-ROLES                                       |
| PII protection in cloud (27018)      | Protect personally identifiable information processed in public cloud        | Field visibility matrix; ENC2 sensitive encryption; private documents bucket; EU regions; leak-path PII redact; no product secondary use of HR PII                          | Implemented              | EV-VISIBILITY, EV-CRYPTO-FIELD, EV-DOCUMENTS                                    |
| PII return / erasure (27018 / 27701) | Support return, transfer, or erasure of PII when contract ends or on request | Org deletion cascade; per-employee DSAR export + in-place anonymization (legal-hold gate); retention purge job request                                                      | Implemented              | EV-ORG-DELETE, EV-RETENTION                                                     |
| Privacy technical controls (27701)   | Support PIMS technical measures for processors/controllers                   | Visibility, retention purge, DSAR, Trust Center, ESS field_consent + My preferences, Art.30 processor register. Controller PIMS / AIPD remain Customer (not a product gap)  | Implemented              | EV-PROC-NEWHIRE, EV-VISIBILITY                                                  |
| Functional suitability (25010)       | Provide correct, complete HRIS capabilities for stated needs                 | Core HR bitemporal lifecycle, performance, learning, compensation, analytics, integrations — recruitment placeholder                                                        | Partial                  | EV-PROC-NEWHIRE, EV-PROC-PERF, EV-PROC-LEARNING                                 |
| Security & reliability (25010)       | Withstand unauthorized access; behave consistently under load/errors         | Defense-in-depth authz; rate limits; Axiom SIEM; documented backup RPO≤24h / RTO≤4h. Optional Sentry APM is not required for this control                                   | Implemented              | EV-HEADERS-CSP, EV-HOSTING-REGIONS                                              |

[↑ Table of contents](#) · [↑ Languages](#)

## 9. End-to-end processes catalogue

Key HRIS processes, ISO relevance, how to test, and evidence IDs.

| Process                           | Actors                  | Routes / APIs                                                                                    | ISO                 | Test procedure                                                                                                                            | Evidence                          |
|-----------------------------------|-------------------------|--------------------------------------------------------------------------------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| Tenant bootstrap                  | Super Admin             | <code>/su-admin</code> , create-organization, deploy-*, module activation                        | 27001, 27017        | Create demo org; confirm seed schemas; check audit <code>MODULE_ACTIVATION</code>                                                         | EV-RBAC-ROLES, EV-AUDIT-TRAIL     |
| Auth & session                    | All users               | <code>/login</code> , <code>/orgSlug</code> , session-policy, Turnstile                          | 27001, 27017        | Login; verify idle timeout; inspect security headers (HSTS/CSP)                                                                           | EV-TURNSTILE, EV-HEADERS-CSP      |
| MFA enrollment & step-up          | Admin / Super Admin     | <code>/security/mfa</code> , MFA step-up at login, <code>REQUIRE_MFA_FOR_PRIVILEGED_ROLES</code> | 27001, 27017        | Enroll TOTP; complete login step-up to <code>aa12</code> ; with flag on, privileged API returns 403 <code>MFA_REQUIRED</code> without MFA | EV-AUTH-MFA                       |
| Org OIDC SSO                      | Org Admin + IdP         | Org-setup IT Link; <code>/api/auth/org-oidc/*</code>                                             | 27001, 27017        | Configure OIDC; login via IdP; confirm open-redirect hardening                                                                            | EV-SSO-OIDC                       |
| RBAC / roles / HR scope           | Org Admin               | Manage Roles; <code>RequireOrgPermission</code>                                                  | 27001, 27017, 27701 | Assign module permissions; verify denied module returns blocked UI/API                                                                    | EV-RBAC-ROLES                     |
| New hire + employee data request  | HR + candidate          | HR new-hire; <code>/employee-data-request/{token}</code>                                         | 27018, 27701        | Trigger data request; open public link; confirm token hashed at rest; <code>npm run test:employee-data-request</code>                     | EV-PROC-NEWHIRE                   |
| Employee update / termination     | HR                      | HR Self Service employee / termination; bitemporal updates                                       | 27001, 27701        | Update with effective date; terminate; verify history segments                                                                            | EV-PROC-UPDATE, EV-PROC-TERMINATE |
| Self-service change → HR approval | Employee / Manager / HR | <code>/api/self-service/submit-change-request</code>                                             | 27001, 27701        | Submit workflow field change; confirm notification; HR applies                                                                            | EV-PROC-SELFSERVICE               |
| Documents DMS                     | HR / Manager / Employee | <code>/api/documents/*</code> , private <code>documents</code> bucket                            | 27001, 27018, 27701 | Upload doc; attempt unauthorized download (expect deny); authorized stream via file route                                                 | EV-DOCUMENTS                      |
| Field visibility & retention      | Org Admin / SU          | Data Visibility & Retention UI                                                                   | 27018, 27701, 25010 | Set manager/employee visibility; set retentionMonths; run analyze/purge                                                                   | EV-VISIBILITY, EV-RETENTION       |
| Mass upload commit / rollback     | HR / Admin              | Mass upload APIs; audit events                                                                   | 27001, 25010        | Commit CSV batch; rollback; verify audit + temporal restore                                                                               | EV-PROC-MASSUPLOAD                |
| Performance campaign cycle        | HR / Manager / Employee | Performance campaigns, documents, sign, push Core HR                                             | 25010, 27001        | <code>npm run test:performance-smoke</code> (live org) or unit tests under <code>lib/performance/__tests__</code>                         | EV-PROC-PERF                      |
| Learning & attestations           | Admin / Learner /       | Learning admin, player, compliance cron                                                          | 25010, 27001        | Enroll; complete SCORM/attestation; check team                                                                                            | EV-PROC-LEARNING                  |

| Process               | Actors                                                   | Routes / APIs                                    | ISO                 | Test procedure                                                                                                     | Evidence                   |
|-----------------------|----------------------------------------------------------|--------------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------|
|                       | Manager                                                  |                                                  |                     | compliance dashboard                                                                                               |                            |
| Integrations export   | Org Admin / M2M                                          | /api/integrations/export, SFTP, HMAC, rate limit | 27001, 27017, 27018 | Regenerate key (once-only plaintext); export with Bearer + HMAC signed by that key; confirm audit fingerprint only | EV-INTEGRATIONS            |
| Proxy / impersonation | SU with active 48h org grant, or Org Admin / HR in scope | /api/proxy/*, /api/su-org-access                 | 27001, 27017        | Request/approve SU access; Enter org; start proxy; JWT remains real user; audit dual identity                      | EV-PROXY, EV-SU-ORG-ACCESS |
| Org deletion cascade  | Super Admin                                              | /api/admin/delete-organization                   | 27701, 27018        | On disposable org only: delete; confirm tenant data + audit purged                                                 | EV-ORG-DELETE              |
| Audit trail review    | Org Admin / SU                                           | Org-setup / SU Audit Trail tab                   | 27001, 27701        | Filter events; export CSV; verify proxy dual identity rows                                                         | EV-AUDIT-TRAIL             |

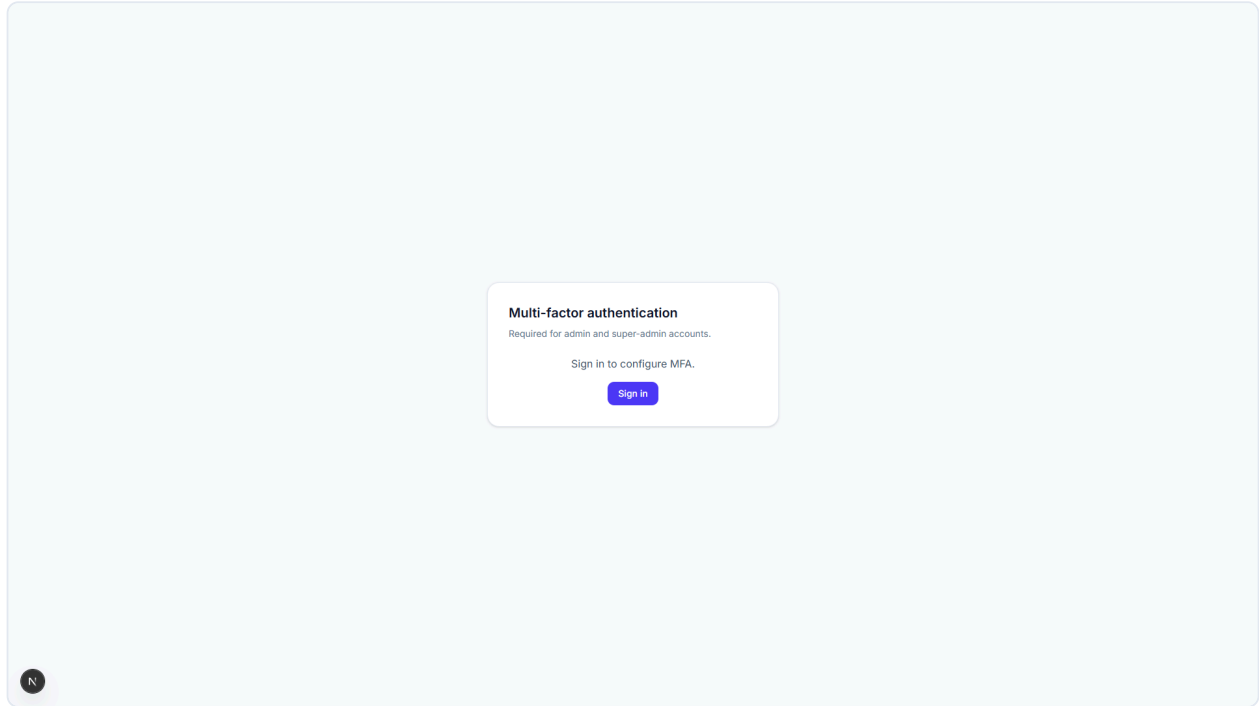
[↑ Table of contents](#) · [↑ Languages](#)

## 10. Evidence pack — how to prove it

Each Evidence ID: what to show, how to test, code references, and a figure slot (replace SVG placeholders with production screenshots per `docs/iso-evidence-capture-checklist.md`).

## EV-AUTH-MFA — MFA TOTP & privileged step-up

- **Show:** Page `/security/mfa`; login MFA challenge; Vercel env `REQUIRE_MFA_FOR_PRIVILEGED_ROLES`
- **Test:** Enroll authenticator; complete step-up to JWT `aa12`; call privileged API without MFA → 403 `MFA_REQUIRED`
- **Code / config:** `lib/auth-mfa-policy.ts`, `lib/mfa-step-up.ts`, `app/security/mfa/page.tsx`



EV-AUTH-MFA — MFA TOTP & privileged step-up (screenshot)

## EV-PASSWORD-POLICY — Password length & complexity messaging

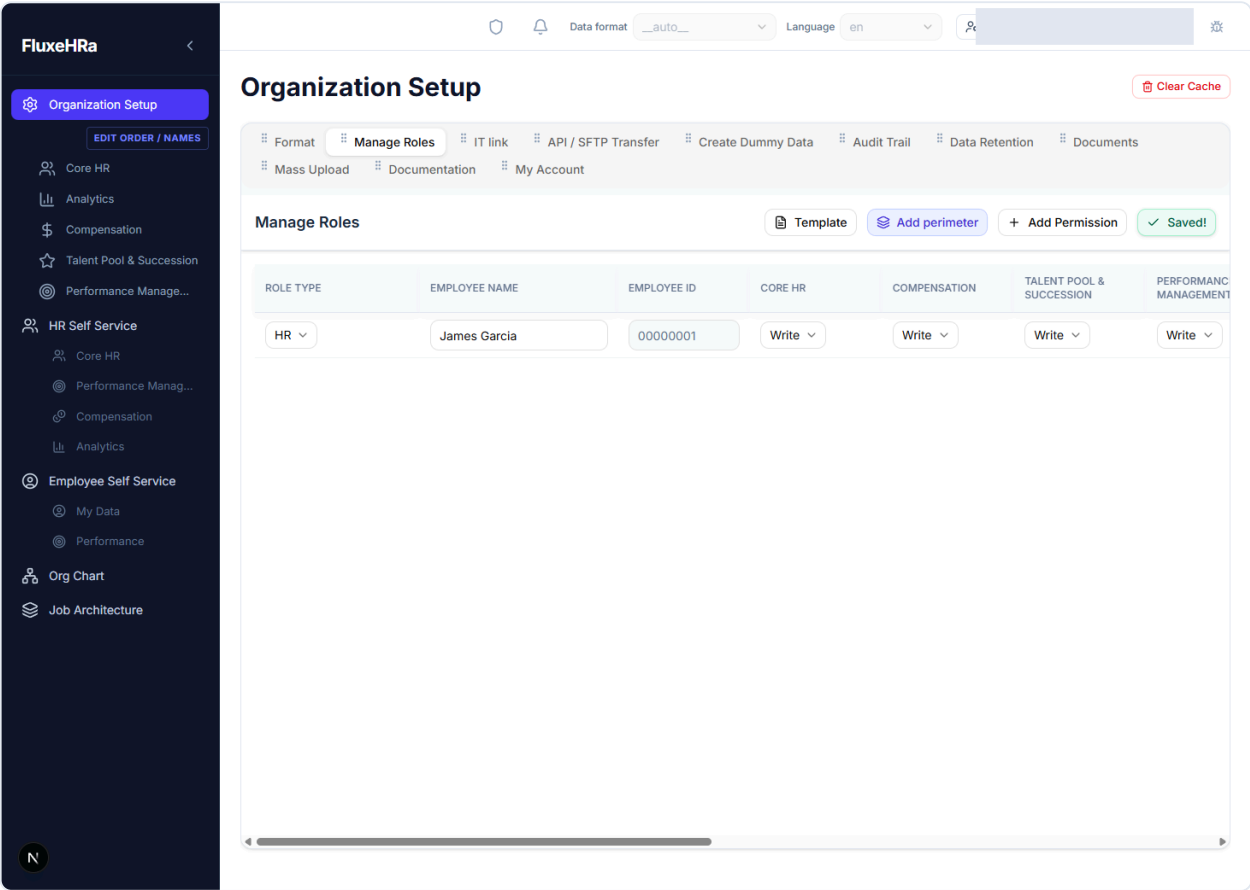
- **Show:** Login → Forgot password notice; `/reset-password` form; welcome/reset emails
- **Test:** Reject short/weak password on set/reset; existing passwords continue to work until changed
- **Code / config:** `lib/password-policy.ts`, `app/reset-password/page.tsx`, `components/sign-in-panel.tsx`, `lib/templated-auth-email.ts`

The screenshot shows a web browser window with the URL `fluxehra.fr`. The page is titled "FluxeHRa" and displays a "Reset password" form. The form includes a "Back to sign in" link, a message about email delivery, a password complexity requirement (12 characters, uppercase, lowercase, digit, and special character), an "Email address" input field with the placeholder `you@company.com`, a "Success!" message with a green checkmark, a "Send reset link" button, and links for "Privacy Policy", "Terms of Use", and "Trust Center". A Cloudflare logo is also visible in the bottom right corner of the form.

EV-PASSWORD-POLICY — Password length & complexity messaging (screenshot)

EV-RBAC-ROLES — Role & permission matrix

- **Show:** Org-setup → Manage Roles; SU Admin org/admins
- **Test:** Remove module write; confirm UI gate and API 403
- **Code / config:** lib/org-permissions.ts , components/manage-roles-tab.tsx , lib/supabase-api-auth.ts



EV-RBAC-ROLES — Role & permission matrix (screenshot)

## EV-RLS-TENANT — Multi-tenant RLS isolation

- **Show:** Attempt cross-org data access (second org user)
- **Test:** Query/API against foreign `organization_id` returns empty/denied; review RLS migrations
- **Code / config:** `supabase/migrations/20260606120000_*`, `20260610120000_*`, `scripts/sql/rls-inventory.sql`

EV-RLS-TENANT

### Multi-tenant RLS isolation

```
Tenant boundary: organization_id enforced in Postgres RLS policies.
Inventory helper: scripts/sql/rls-inventory.sql

-- Read-only RLS inventory (plan "Remédiation sécurité juin 2026", item 9).
-- Run in Supabase Dashboard > SQL Editor (or psql) on project zlsruhdxyfwqfpzckg.
-- No writes are performed.

-- 1. RLS enabled / forced per table (public schema)
select
  n.nspname as schema,
  c.relname as table name,
  c.relrowsecurity as rls_enabled,
  c.relforcerowsecurity as rls_forced
from pg_class c
join pg_namespace n on n.oid = c.relnamespace
where n.nspname = 'public'
and c.relkind = 'r'
order by c.relname;

-- 2. All policies on public tables
select
  schemaname,
  tablename,
  policyname,
  permissive,
  roles,
  cmd,
  qual,
  with_check
from pg_policies
where schemaname = 'public'
order by tablename, policyname;

-- 3. Focus: legacy tables flagged by the June 2026 audit
select
  tablename,
  policyname,
  permissive,
```

Generated evidence card — FluxeHra ISO Alignment Pack

EV-RLS-TENANT — Multi-tenant RLS isolation (screenshot)

## EV-CRYPTO-FIELD — Sensitive field encryption

- **Show:** Save SSN/IBAN; inspect DB value prefix `ENC2::`
- **Test:** Encrypt/decrypt via authorized role; non-privileged decrypt limited to own/team ciphertext
- **Code / config:** `lib/encryption-core.ts`, `app/api/crypto/*`, `lib/crypto-route-auth.ts`

EV-CRYPTO-FIELD

### Sensitive field encryption (ENC2::)

```
Application ciphertext prefix: ENC2:: (AES-GCM)
Source: lib/encryption-core.ts
Decrypt gated by role / ownership (lib/crypto-route-auth.ts)

Demo note: never capture plaintext SSN/IBAN in customer packs.
DB inspection should show only ENC2::... values for sensitive columns.
```

Generated evidence card — FluxeHRa ISO Alignment Pack

EV-CRYPTO-FIELD — Sensitive field encryption (screenshot)

EV-AUDIT-TRAIL — Audit trail UI

- **Show:** Org-setup / SU → Audit Trail
- **Test:** Perform audited action (mass upload, settings); confirm event row; CSV export
- **Code / config:** lib/audit-server.ts, lib/audit-client.ts, components/audit-trail-tab.tsx

FluxeHRa

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Organization Setup

Format

Manage Roles

IT link

API / SFTP Transfer

Create Dummy Data

Audit Trail

Data Retention

Documents

Mass Upload

Documentation

My Account

Audit Trail

mm/dd/yyyy

to

mm/dd/yyyy

Search logs...

Compliance evidence

Export CSV

| DATE & TIME           | PAGE / MODULE                               | ACTION (REASON) | DETAILS                                         |
|-----------------------|---------------------------------------------|-----------------|-------------------------------------------------|
| Aug 10, 2026 17:18:29 | /fluxehra/org-se<br>tup                     | PAGE_VIEW       | Visited /fluxehra/org-setup                     |
| Aug 10, 2026 17:14:15 | /fluxehra/hr-self<br>-service/core-hr       | PAGE_VIEW       | Visited /fluxehra/hr-self-<br>service/core-hr   |
| Aug 10, 2026 17:14:03 | /fluxehra/org-se<br>tup                     | PAGE_VIEW       | Visited /fluxehra/org-setup                     |
| Aug 10, 2026 17:13:50 | /fluxehra/hr-self<br>-service/docum<br>ents | PAGE_VIEW       | Visited /fluxehra/hr-self-<br>service/documents |
| Aug 7, 2026 22:32:50  | /fluxehra/hr-self<br>-service/docum<br>ents | PAGE_VIEW       | Visited /fluxehra/hr-self-<br>service/documents |
| Aug 7, 2026 22:32:43  | /fluxehra/hr-self<br>-service/core-hr       | PAGE_VIEW       | Visited /fluxehra/hr-self-<br>service/core-hr   |
| Aug 7, 2026 22:32:28  | /fluxehra/org-ch<br>art                     | PAGE_VIEW       | Visited /fluxehra/org-chart                     |
| Aug 7, 2026 22:17:18  | /fluxehra/org-ch<br>art                     | PAGE_VIEW       | Visited /fluxehra/org-chart                     |
| Aug 7, 2026 22:15:16  | /fluxehra/org-ch<br>art                     | PAGE_VIEW       | Visited /fluxehra/org-chart                     |

Showing 1-20 of 339

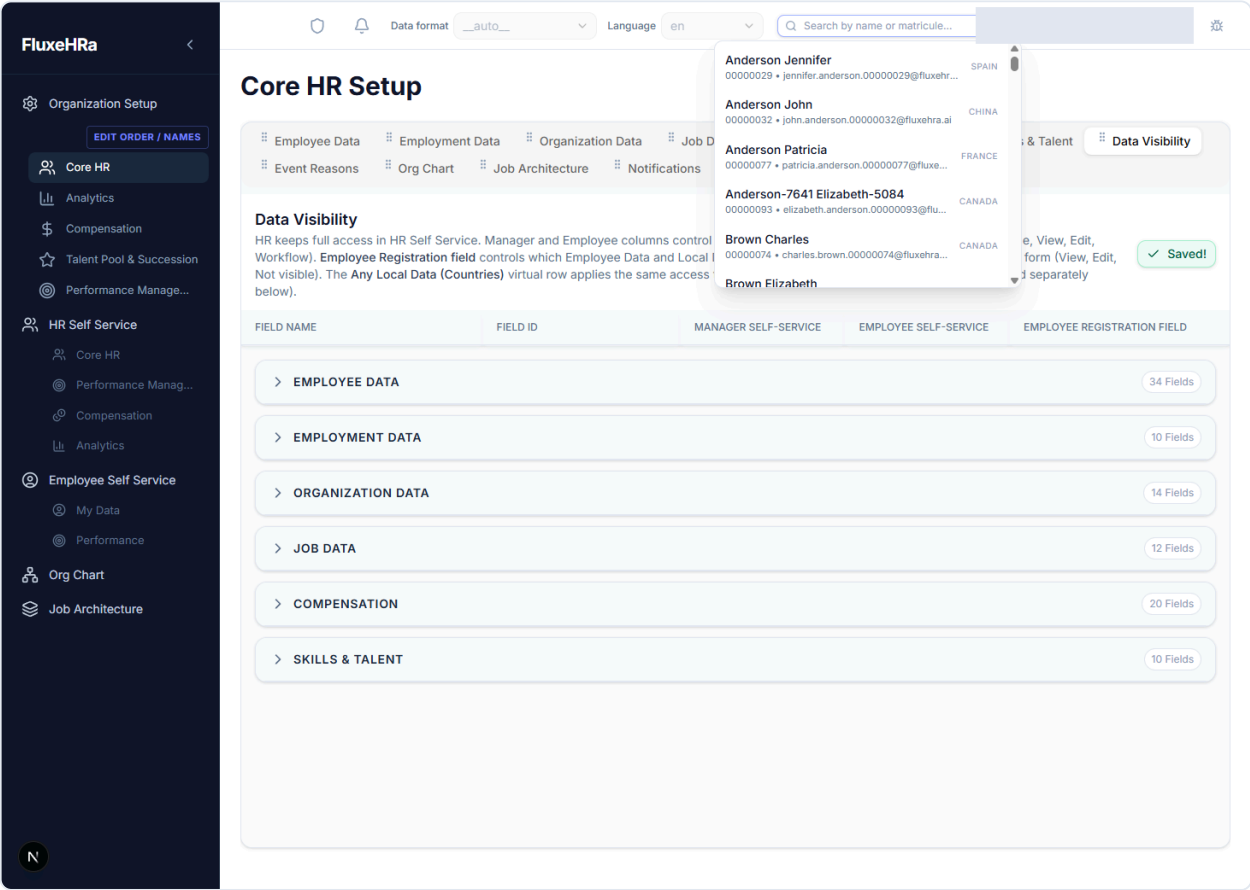
Per page 20

< 1 2 3 ... 17 >

EV-AUDIT-TRAIL — Audit trail UI (screenshot)

EV-PROXY — Proxy accountability

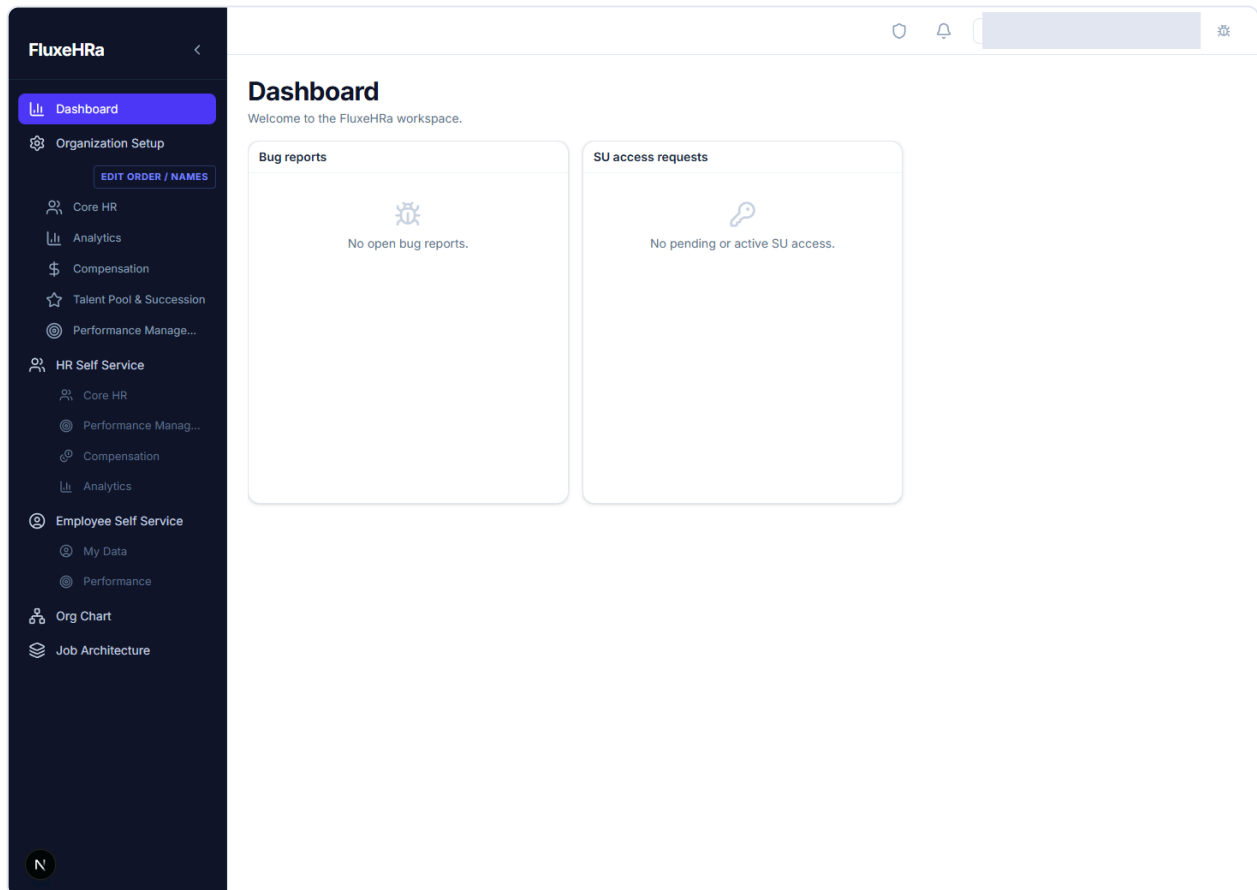
- **Show:** Proxy session banner; audit with proxied identity
- **Test:** With active SU grant (or org privileged role): start/end proxy; confirm continuous eligibility re-check; dual identity in logs
- **Code / config:** `lib/proxy-server.ts`, `lib/proxy-api-guard.ts`, `lib/su-org-access.ts`



EV-PROXY — Proxy accountability (screenshot)

## EV-SU-ORG-ACCESS — SU org access grants (48h)

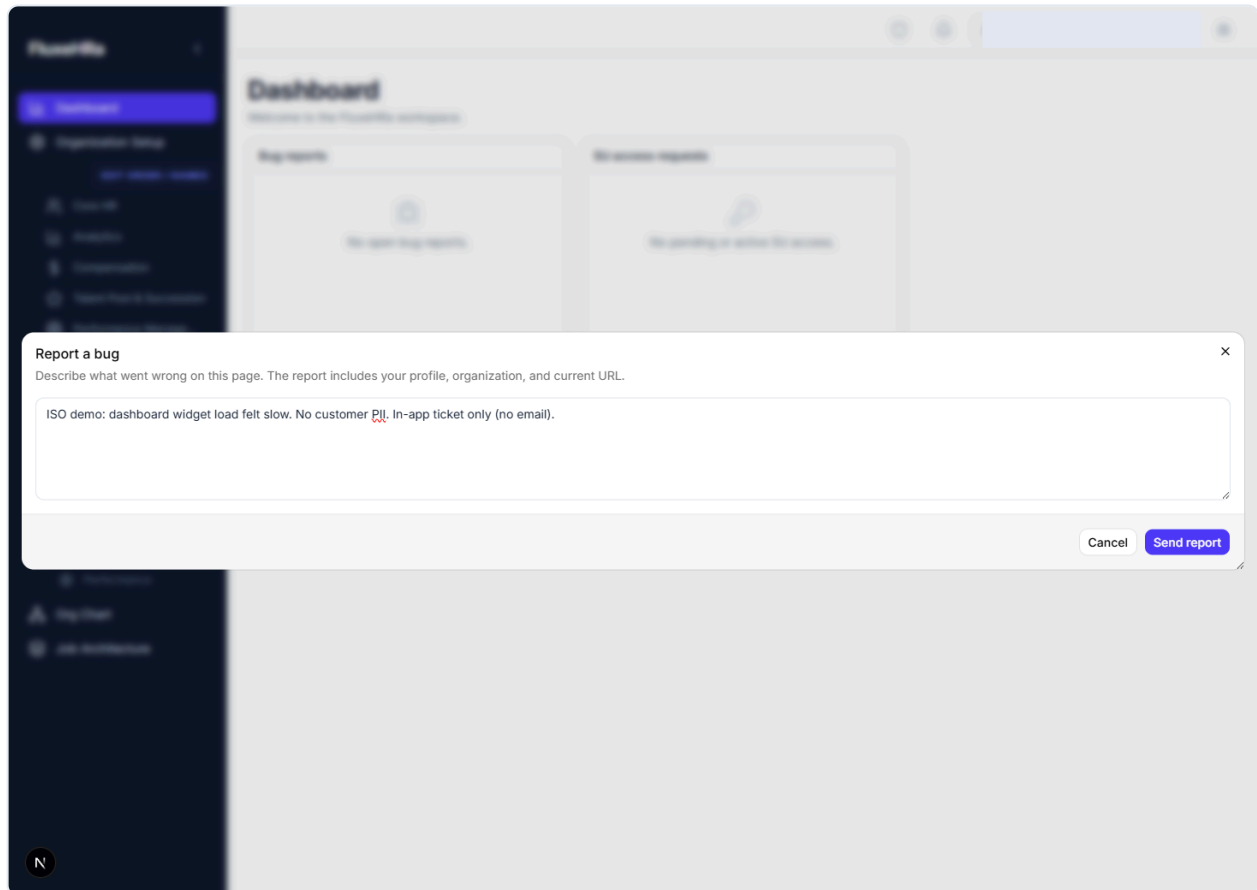
- **Show:** SU Enter Organisation → Request; Org Admin Dashboard → Accept/Deny; emerald authorized orgs
- **Test:** Approve grant; Enter org; confirm middleware/API deny without grant for data paths; expire after 48h kicks SU out. Deploy-schema to orgs does NOT require grant (config only, no PII read).
- **Code / config:** `su_org_access_grants` , `/api/su-org-access` , `has_active_su_org_grant`



EV-SU-ORG-ACCESS — SU org access grants (48h) (screenshot)

## EV-BUG-ESCALATION — Manual bug escalation

- **Show:** Report a bug → HR / Org Admin / SU Dashboard widgets
- **Test:** Submit manual bug (ticket, no email); Forward HR→Admin→SU; Clear; auto client errors still email SMTP
- **Code / config:** `bug_report_tickets`, `/api/bug-report`, `/api/bug-reports`



EV-BUG-ESCALATION — Manual bug escalation (screenshot)

EV-VISIBILITY — Data visibility matrix

- **Show:** Core HR / Data Visibility; ESS field hidden vs HR visible
- **Test:** Set field to `none` for employee; confirm self-service omit/deny
- **Code / config:** `lib/field-visibility.ts`, `lib/self-service-submit-auth.ts`

FluxeHRA

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Data format

\_\_auto\_\_

Language

en

Core HR Setup

Employee Data

Employment Data

Organization Data

Job Data

Compensation

Local Data

Skills & Talent

Data Visibility

Event Reasons

Org Chart

Job Architecture

Notifications

Data Visibility

HR keeps full access in HR Self Service. Manager and Employee columns control Manager Self Service and Employee Self Service (None, View, Edit, Workflow). Employee Registration field controls which Employee Data and Local Data fields appear on the hired-employee data request form (View, Edit, Not visible). The Any Local Data (Countries) virtual row applies the same access to every country-specific Local Data schema (not listed separately below).

✓ Saved!

| FIELD NAME          | FIELD ID | MANAGER SELF-SERVICE | EMPLOYEE SELF-SERVICE | EMPLOYEE REGISTRATION FIELD |
|---------------------|----------|----------------------|-----------------------|-----------------------------|
| > EMPLOYEE DATA     |          |                      |                       | 34 Fields                   |
| > EMPLOYMENT DATA   |          |                      |                       | 10 Fields                   |
| > ORGANIZATION DATA |          |                      |                       | 14 Fields                   |
| > JOB DATA          |          |                      |                       | 12 Fields                   |
| > COMPENSATION      |          |                      |                       | 20 Fields                   |
| > SKILLS & TALENT   |          |                      |                       | 10 Fields                   |

EV-VISIBILITY — Data visibility matrix (screenshot)

EV-RETENTION — Retention configuration & purge

- **Show:** Retention months per field; document type retention; analyze/purge actions
- **Test:** Configure retention; run Retention analysis; purge expired values; confirm RETENTION\_\* audit events
- **Code / config:** `lib/retention-purge.ts`, `/api/hr/retention`, field-visibility retention tab

FluxeHRa

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Organization Setup

Clear Cache

FormatManage RolesIT linkAPI / SFTP TransferCreate Dummy DataAudit TrailData RetentionDocuments

Mass UploadDocumentationMy Account

Data Retention

Retention analysis

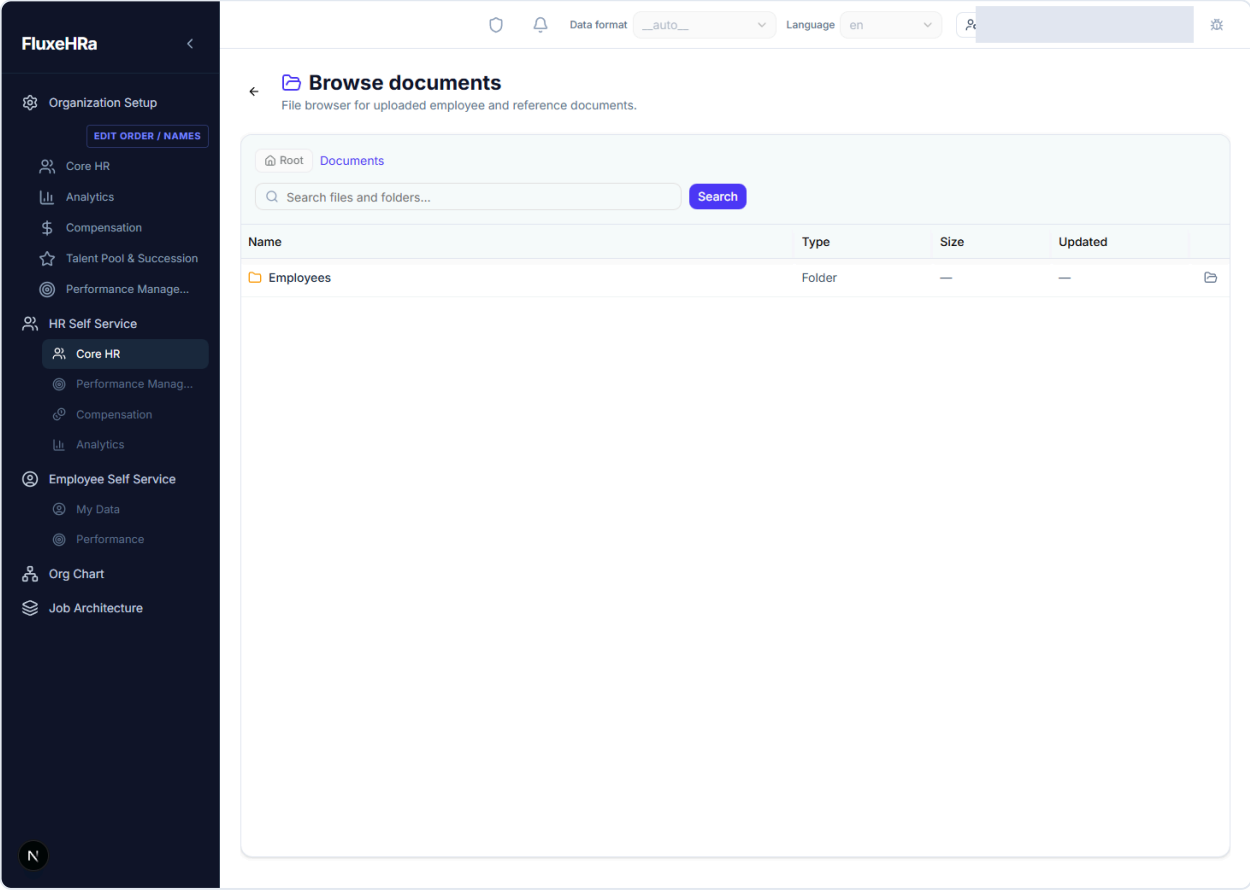
✓ Saved!

| FIELD NAME          | FIELD ID | RETENTION LENGTH (MONTHS AFTER DEPARTURE) | NUMBER OF ITEMS |
|---------------------|----------|-------------------------------------------|-----------------|
| CORE HR             |          |                                           |                 |
| > EMPLOYEE DATA     |          |                                           | 34 Fields       |
| > EMPLOYMENT DATA   |          |                                           | 10 Fields       |
| > ORGANIZATION DATA |          |                                           | 14 Fields       |
| > JOB DATA          |          |                                           | 12 Fields       |
| > COMPENSATION      |          |                                           | 20 Fields       |
| > SKILLS & TALENT   |          |                                           | 10 Fields       |
| ANALYTICS           |          |                                           |                 |
| > ANALYTICS         |          |                                           | 0 Fields        |
| COMPENSATION        |          |                                           |                 |

EV-RETENTION — Retention configuration & purge (screenshot)

EV-DOCUMENTS — Private document access

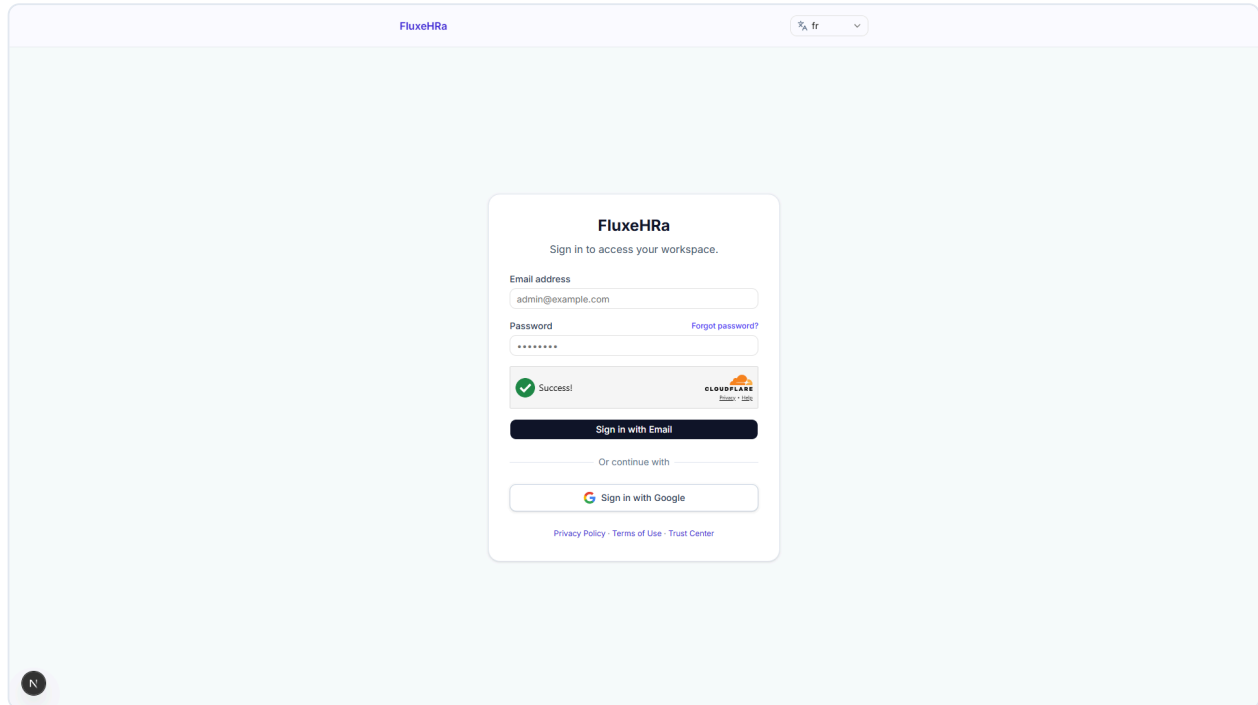
- **Show:** Upload under employee; download via app only
- **Test:** Direct storage URL without auth fails; authorized `/api/documents/file/...` succeeds; scoped HR denied outside regional perimeter on direct URL
- **Code / config:** `lib/document-access.ts`, `lib/storage-ops.ts`, migration documents bucket private



EV-DOCUMENTS — Private document access (screenshot)

## EV-TURNSTILE — Bot protection (Turnstile)

- **Show:** SU System Setup / Org IT Link Turnstile toggle; login challenge
- **Test:** Enable Turnstile; blocked without token on check-email / forgot-password
- **Code / config:** `lib/turnstile-server.ts`, `lib/turnstile-settings.ts`



EV-TURNSTILE — Bot protection (Turnstile) (screenshot)

## EV-SSO-OIDC — Organization OIDC SSO

- **Show:** Org-setup → IT Link SSO settings
- **Test:** Authorize + callback with HMAC state; invalid redirect rejected
- **Code / config:** `app/api/auth/org-oidc/*`, `lib/org-oidc-state.ts`, `lib/app-origin.ts`

The screenshot displays the FluxeHRA web application interface. On the left is a dark sidebar with a navigation menu. The main content area is titled "Organization Setup" and features a top navigation bar with various settings tabs. The "IT link" tab is currently selected. Below the tabs, there are several configuration sections: "Time out for Disconnecting in minutes" set to 60, "Turnstile Captcha" which is disabled, and "SMTP" settings. The "OIDC SSO" section is expanded, showing a toggle switch that is currently "Off". Below the toggle, there are input fields for "Issuer (OIDC)" (containing "https://login.microsoftonline.com/.../v2.0"), "Authorization endpoint", "Token endpoint", and "JWKS URI". A "Clear Cache" button is located in the top right corner of the main content area.

**FluxeHRA**

**Organization Setup** Clear Cache

**IT link** | Format | Manage Roles | API / SFTP Transfer | Create Dummy Data | Audit Trail | Data Retention | Documents | Mass Upload | Documentation | My Account

Time out for Disconnecting in minutes : ☐ 60

**Turnstile Captcha** ☐ Require Cloudflare Turnstile on this organization's sign-in page. Uses keys from SU Admin → System Setup.

**SMTP** ☐ Outgoing mail for this organization (invites, notifications, etc.).

**OIDC SSO** ☐ OpenID Connect single sign-on for members of this organization (not Super Admin). Register the redirect URI below with your IdP.  
Redirect URI: `http://localhost:3000/api/auth/org-oidc/callback`

**Off**

**Issuer (OIDC)**

**Authorization endpoint**

**Token endpoint**

**JWKS URI**

EV-SSO-OIDC — Organization OIDC SSO (screenshot)

## EV-ESIGN-FLUXEHRA — Fluxehra e-signature (eIDAS SES + optional PAdES-B)

- **Show:** SU Setup platform toggle; Org IT Link (expiry, OTP, consent, company signatories); public `/sign/[token]`; HR evidence Certificate/JSON; optional PAdES seal
- **Test:** Send envelope; open link; OTP if required; consent; draw/type; complete stamped PDF; download SES evidence pack; exclusivity disables DocuSign; optional PAdES-B `ETSI.CAdES.detached`
- **Code / config:** `lib/esign/*`, `lib/esign-provider.ts`, `docs/esign-standards.md`, `app/api/public/esign/*`, migrations through `20260929210000_esign_audit_pades.sql`

### Evidence placeholder

EV-ESIGN-FLUXEHRA

Replace with screenshot — see `docs/iso-evidence-capture-checklist.md`

FluxeHRa ISO Alignment Pack

EV-ESIGN-FLUXEHRA — Fluxehra e-signature (eIDAS SES + optional PAdES-B) (placeholder)

## EV-DOCUSIGN — DocuSign e-signature (optional)

- **Show:** SU Setup DocuSign + Org IT Link Account/User ID + Grant consent
- **Test:** Sandbox send + Connect completed webhook; exclusivity disables Fluxehra e-signature
- **Code / config:** `lib/docusign-*.ts`, `app/api/hr/docusign/*`, `/api/integrations/docusign/webhook`

### Evidence placeholder

EV-DOCUSIGN

Replace with screenshot — see docs/iso-evidence-capture-checklist.md

FluxeHRa ISO Alignment Pack

EV-DOCUSIGN — DocuSign e-signature (optional) (placeholder)

## EV-INTEGRATIONS — Integration export security

- **Show:** Org-setup → API / SFTP; regenerate key once
- **Test:** Export with Bearer integration key + HMAC headers (per-key secret); rate limit; audit stores fingerprint not payload
- **Code / config:** `lib/integration-api-key.ts`, `lib/integration-export-*.ts`

The screenshot shows the FluxeHRA web application interface. On the left is a dark sidebar with the 'FluxeHRA' logo and a menu of options including 'Organization Setup' (highlighted), 'Core HR', 'Analytics', 'Compensation', 'Talent Pool & Succession', 'Performance Manage...', 'HR Self Service', 'Employee Self Service', 'Org Chart', and 'Job Architecture'. The main content area is titled 'Organization Setup' and features a 'Clear Cache' button. Below the title is a navigation bar with tabs: 'Format', 'Manage Roles', 'IT link', 'API / SFTP Transfer' (selected), 'Create Dummy Data', 'Audit Trail', 'Data Retention', 'Documents', 'Mass Upload', 'Documentation', and 'My Account'. The 'API / SFTP Transfer' tab is active, showing a 'New API / SFTP' section with a '+ New API Key' button. The main configuration area is titled 'API Credentials & Webhook' and includes fields for 'Integration Name' (set to 'New API Key'), 'API key' (displaying 'fx\_M6EK...Z0VD' with a 'Renew key' button), 'Export IP allowlist (optional)' (set to '203.0.113.10, 198.51.100.0'), 'Push Destination (Webhook)' (set to 'https://api.external-system.com/webhook/hr'), and 'Data Transfer Type' (with options for 'Full Transfer' and 'Incremental Transfer'). A 'Saved!' status is visible in the top right of the configuration area.

EV-INTEGRATIONS — Integration export security (screenshot)

## EV-HEADERS-CSP — Security headers & CSP

- **Show:** Browser DevTools → Response headers on any authenticated page
- **Test:** Confirm CSP nonce, HSTS, X-Frame-Options DENY, nosniff
- **Code / config:** `lib/csp.ts`, `proxy.ts`, `next.config.js`

EV-HEADERS-CSP

### Security response headers

```
GET http://127.0.0.1:3000/trust
status: 200

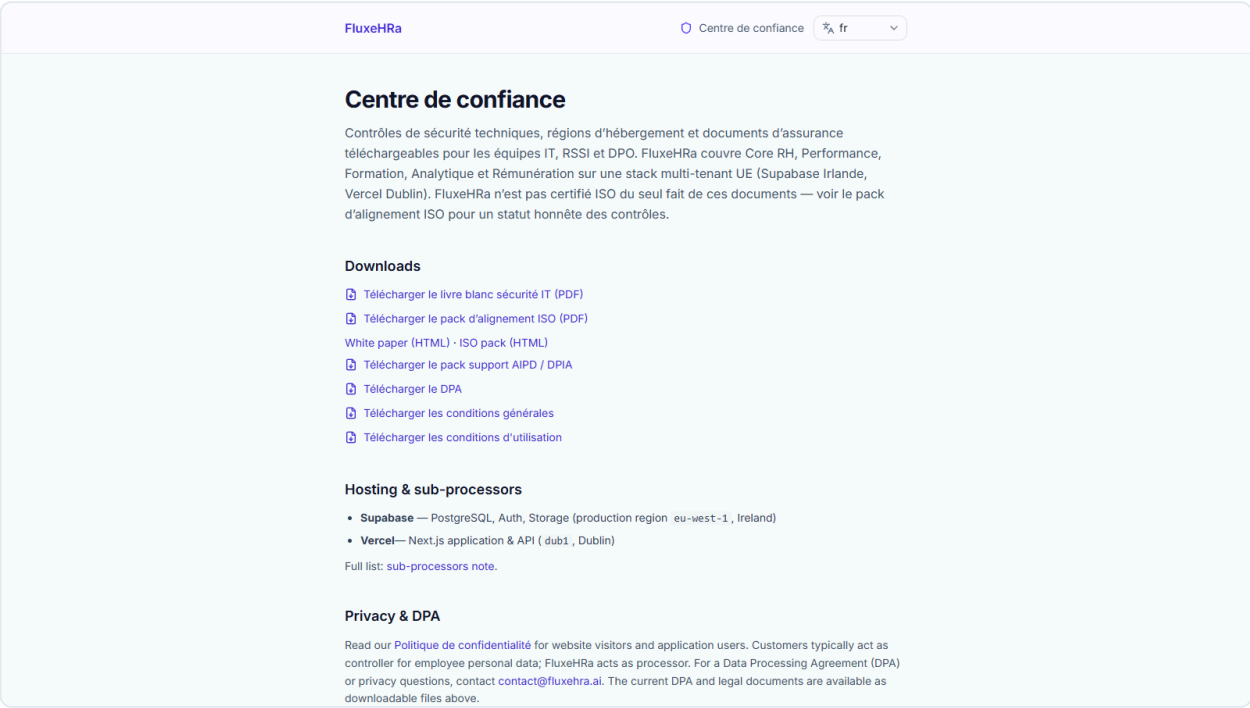
content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'
https://challenges.cloudflare.com https://va.vercel-scripts.com; style-src 'self' 'unsafe-
inline'; img-src 'self' data: blob: https://*.supabase.co; font-src 'self' data; connect-src
'self' https://*.supabase.co wss://*.supabase.co https://challenges.cloudflare.com
https://vitals.vercel-insights.com; frame-src 'self' https://challenges.cloudflare.com; object-
src 'none'; base-uri 'self'; form-action 'self'; frame-ancestors 'none'
strict-transport-security: max-age=63072000; includeSubDomains; preload
x-frame-options: DENY
x-content-type-options: nosniff
referrer-policy: strict-origin-when-cross-origin
permissions-policy: camera=(), microphone=(), geolocation=(), payment=()
x-dns-prefetch-control: on
```

Generated evidence card — FluxeHRa ISO Alignment Pack

EV-HEADERS-CSP — Security headers & CSP (screenshot)

EV-HOSTING-REGIONS — EU hosting alignment

- **Show:** Supabase project region; `vercel.json` region `dub1`
- **Test:** Document eu-west-1 + dub1 in customer processing register
- **Code / config:** `vercel.json`, `.env.example`, security whitepaper § hosting



EV-HOSTING-REGIONS — EU hosting alignment (screenshot)

EV-PROC-NEWHIRE — New hire & data request

- **Show:** HR Self Service → New Hire; public token page
- **Test:** `npm run test:employee-data-request`; manual 90-day token expiry
- **Code / config:** `lib/employee-data-request-*.ts`, public EDR APIs

FluxeHra

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Data format

\_\_auto\_\_

Language

en

New Hire (Manual)

Create a new employee record across all schemas.

Save as draft

Request Hired Employee Data

Complete Hire

Contract for signature

Select employee country first

Preview

Send for Signature

Event Details

Effective Date (Hire Date) \*

08/10/2026

Event Reason \*

NEW\_HIRE

Country \*

Select Country

EMPLOYEE DATA

34 Fields

EMPLOYMENT DATA

10 Fields

ORGANIZATION

14 Fields

JOB DATA

12 Fields

COMPENSATION

20 Fields

EV-PROC-NEWHIRE — New hire & data request (screenshot)

EV-PROC-UPDATE — Bitemporal employee update

- **Show:** HR employee record with effective dating
- **Test:** Split history on mid-period change; verify prior segment retained
- **Code / config:** lib/temporal-data.ts

FluxeHRa

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

N

🛡️

🔔

Data format: \_\_auto\_\_

Language: en

🔍

←

ID: 00000014 • Status: Active

Export DSAR

Anonymize

<

>

History

Current (2026-08-10)

Save Changes

> EMPLOYEE DATA

34 Fields

> EMPLOYMENT DATA

10 Fields

> ORGANIZATION

14 Fields

> JOB DATA

12 Fields

> COMPENSATION

20 Fields

> LOCAL DATA

6 Fields

> SKILLS & TALENT

10 Fields

EV-PROC-UPDATE — Bitemporal employee update (screenshot)

## EV-PROC-TERMINATE — Termination

- **Show:** HR Self Service → Termination
- **Test:** Set end dates/status; confirm lifecycle event
- **Code / config:** HR termination route under `hr-self-service/termination`

The screenshot displays the 'Employee Termination' process in the FluxeHRA system. The interface is divided into a left sidebar and a main content area. The sidebar, titled 'FluxeHRA', contains a navigation menu with categories like 'Organization Setup', 'HR Self Service', 'Employee Self Service', 'Org Chart', and 'Job Architecture'. The 'HR Self Service' category is expanded, showing 'Core HR' as the selected option. The main content area features a header with 'Employee Termination' and a sub-header 'Process an employee departure.' A 'Process Termination' button is located in the top right. Below the header, there is a 'Select Employee' section with a search bar labeled 'Search Active Employees...'. The 'Termination Details' section contains two fields: 'Effective Date' with a date picker set to '08/10/2026' and 'Termination Reason' with a dropdown menu set to 'RESIGNATION' under the 'Category: Termination' label.

FluxeHRA

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

N

Employee Termination

Process an employee departure.

Process Termination

Select Employee

Search Active Employees...

Termination Details

Effective Date \*

08/10/2026

Termination Reason \*

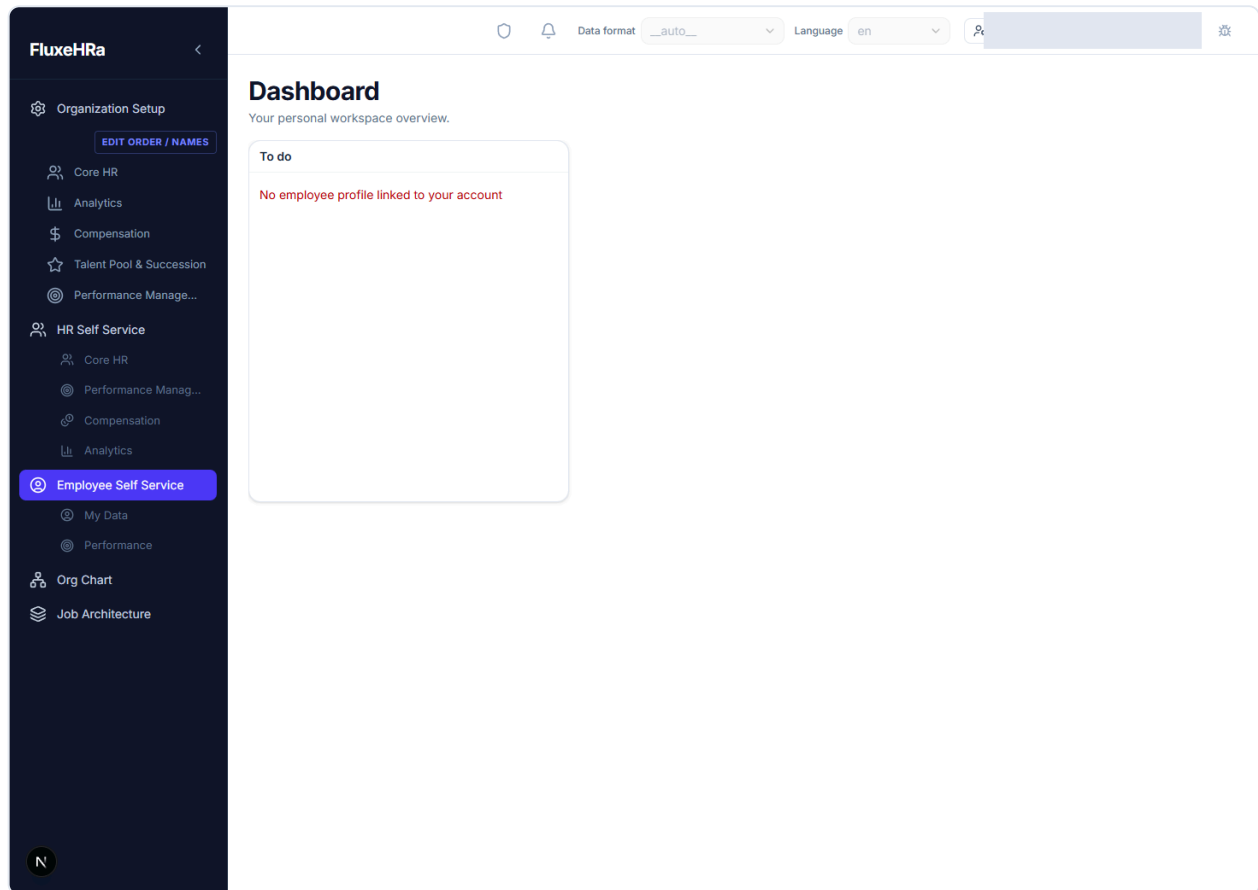
Category: Termination

RESIGNATION

EV-PROC-TERMINATE — Termination (screenshot)

## EV-PROC-SELFSERVICE — Self-service change request

- **Show:** My Data / My Team workflow fields; HR notification
- **Test:** Submit change; approve/apply as HR
- **Code / config:** `lib/self-service-submit-auth.ts`



EV-PROC-SELFSERVICE — Self-service change request (screenshot)

EV-PROC-MASSUPLOAD — Mass upload & rollback

- **Show:** Mass Upload tab; batch list
- **Test:** Commit then delete/rollback batch; audit events present
- **Code / config:** `/api/admin/mass-upload/*`

FluxeHRa

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Organization Setup

Clear Cache

Format

Manage Roles

IT link

API / SFTP Transfer

Create Dummy Data

Audit Trail

Data Retention

Documents

Mass Upload

Documentation

My Account

Mass Upload for a Domain

Upload a full module slice (all uploadable fields) for existing employees. For Core HR, one file covers all schema tabs except Local Data (use the per-tab flow if you need local country-specific fields). CSV headers use field IDs; include `employee_id` with the in-app Employee ID (not the Supabase UUID).

Upload name

Domain (module)

Effective date

Event category

Sub-reason

Q1 job data refresh

Core HR

08/10/2026

Hire / Rehire

NEW\_HIRE

Same-day order

First

Last

Download sample

Browse CSV

Upload & save

Mass Upload for specific field(s)

Pick one or more fields; the sample CSV always includes `employee_id` for matching.

Upload name

Domain (module)

Schema tab

Effective date

Event category

Salary correction batch

Core HR

employee-data

08/10/2026

Hire / Rehire

Sub-reason

NEW\_HIRE

Fields

Select field

Add field

Same-day order

First

Last

Download sample

Browse CSV

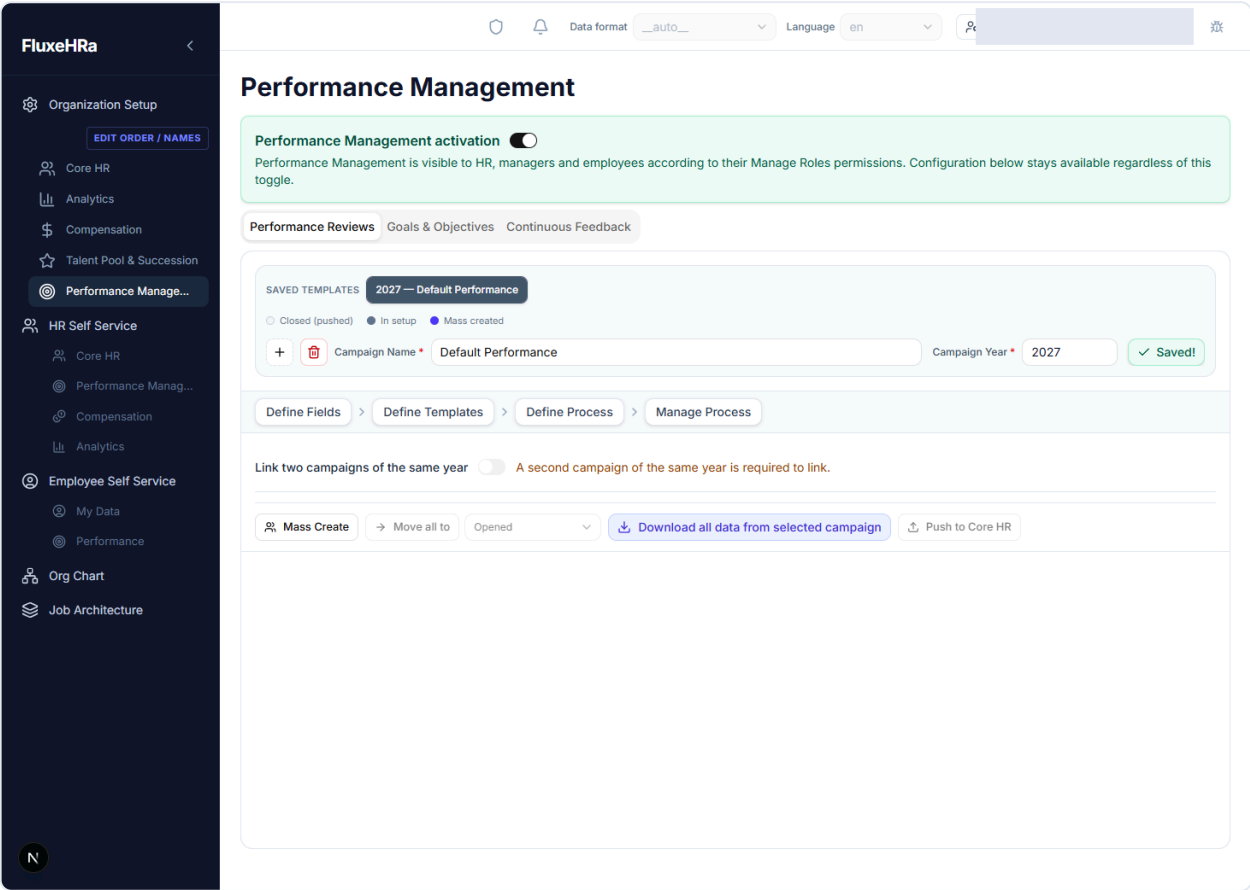
Upload & save

Delete a Mass Upload for a Domain

EV-PROC-MASSUPLOAD — Mass upload & rollback (screenshot)

EV-PROC-PERF — Performance campaign

- **Show:** Performance Management campaign → document → sign
- **Test:** `npm test` (performance unit tests); optional `npm run test:performance-smoke`
- **Code / config:** `lib/performance/` , `app/api/performance/`



EV-PROC-PERF — Performance campaign (screenshot)

## EV-PROC-LEARNING — Learning compliance

- **Show:** Learning admin + team compliance tab
- **Test:** Enroll; progress; attestation; compliance dashboard
- **Code / config:** `app/api/learning/` , `/api/cron/learning-compliance`

### Evidence placeholder

EV-PROC-LEARNING

Replace with screenshot — see docs/iso-evidence-capture-checklist.md

FluxeHRa ISO Alignment Pack

EV-PROC-LEARNING — Learning compliance (placeholder)

## EV-ORG-DELETE — Organization deletion cascade

- **Show:** SU Admin delete organization (disposable org only)
- **Test:** Confirm cascade removes org tables, storage prefixes, member auth users
- **Code / config:** `lib/delete-organization-cascade.ts`

### Evidence placeholder

EV-ORG-DELETE

Replace with screenshot — see docs/iso-evidence-capture-checklist.md

FluxeHRa ISO Alignment Pack

EV-ORG-DELETE — Organization deletion cascade (placeholder)

## EV-SDLC-TESTS — Automated tests & change evidence

- **Show:** CI/local test run output; migration history
- **Test:** `npm test`; `npm run test:employee-data-request`; `npm run lint`; GitHub `security-tests` workflow
- **Code / config:** `lib/__tests__` / , `lib/performance/__tests__` / , `supabase/migrations` / , `.github/workflows/security-tests.yml`

EV-SDLC-TESTS

### Offline security smoke tests

```
$ npm run test:security-smoke  
  
> ai-studio-applet@0.1.0 test:security-smoke  
> npx tsx scripts/test-security-smoke.ts  
security-smoke: password policy  
security-smoke: privileged MFA roles include hr  
security-smoke: MFA policy function callable  
security-smoke: ops observability does not throw  
security-smoke: OK
```

Generated evidence card — FluxehRa ISO Alignment Pack

EV-SDLC-TESTS — Automated tests & change evidence (screenshot)

## EV-SECURITY-WATCH — Security Watch (CERT-FR / CISA / OSV)

- **Show:** Sanitized card: SU Admin Security Watch sources + daily GitHub Action + Dependabot — no operator emails
- **Test:** Run `npm run security:watch`; open SU Admin → Security Watch; confirm daily `security-watch.yml` + Dependabot
- **Code / config:** `lib/security-watch.ts`, `app/api/su-admin/security-watch/route.ts`, `.github/workflows/security-watch.yml`; signed register (private) Certification documentation/policies/Security-community-subscriptions

EV-SECURITY-WATCH

Sanitized — no nominative PII

### Security Watch (CERT-FR / CISA / OSV)

```
ISO A.5.6 — contact with special interest groups
Product: SU Admin + Security Watch (impact-filtered RSS + lockfile)
CLI: npm run security:watch
CI: .github/workflows/security-watch.yml (daily) + Github Dependabot
Sources: CERT-FR avis, CISA KEV, OSV (npm lockfile)
Signed register (private): Security-community-subscriptions — 2026-08-14
Email backups: CERT-FR avis, CISA KEV, vendor status pages (no paid ISAC)
Public pack: no operator emails
```

FluxHra ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SECURITY-WATCH — Security Watch (CERT-FR / CISA / OSV) (screenshot)

## EV-ENV-SEPARATION — Dev / production environment separation

- **Show:** Sanitized card: Git main→prod vs Git dev→Vercel saas-flex-hr-sql-dev + Supabase FluxeHRa-dev (eu-west-1) — no project API keys or full refs
- **Test:** Confirm Vercel-dev Production deployment from dev ; Supabase FluxeHRa-dev Healthy in West EU; no customer PII in Dev
- **Code / config:** README.md deploy tracks; lib/non-prod-env-guard.ts ; private screenshots Certification documentation/ops/EV-ENV-SEPARATION-\*-2026-08-16.png

EV-ENV-SEPARATION

Sanitized — no nominative PII

### Dev / production environment separation

```
ISO A.8.31 — separation of development, test and production
Production: Git main → Vercel saas-flex-hr-sql → Supabase FluxeHRa → fluxehra.ai
Dev: Git dev → Vercel saas-flex-hr-sql-dev → Supabase FluxeHRa-dev (eu-west-1 / West EU Ireland)
Evidence dated 2026-08-16: Vercel-dev Ready from branch dev; FluxeHRa-dev Healthy
Policy: Non-prod-data-policy (signed) — no customer PII dumps in Dev
Runtime: lib/non-prod-env-guard.ts (assertNonProdSupabaseUrl when PRODUCTION_SUPABASE_URL set)
Private full screenshots retained under Certification documentation/ops/
Public pack: no Supabase project refs / service keys
```

FluxeHRa ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-ENV-SEPARATION — Dev / production environment separation (screenshot)

## EV-SIEM-AXIOM — Axiom security SIEM monitors

- **Show:** Sanitized dashboard card: fluxehra\_logs SECURITY\_EVENT monitors — BOLA/tenant, per-IP brute-force, high-signal (cron/RLS/HMAC/SSRF); no query payloads with PII
- **Test:** Confirm three monitors + ingest smoke; private full screenshot retained by Foil Envie
- **Code / config:** lib/security-logger.ts, docs/siem-security-operations.md (internal), docs/subprocessors.md (Axiom)

EV-SIEM-AXIOM

Sanitized — no nominative PII

### Axiom security SIEM monitors

```
Dataset: fluxehra_logs (SECURITY_EVENT)
Monitors (3 slots): BOLA/tenant (403), per-IP brute-force, high-signal (cron/RLS/HMAC/SSRF)
Payload policy: no HR business PII in SIEM events
Edge: us-east-1.aws.edge.axiom.co (event storage/query)
Full operator screenshot: retained privately by Foil Envie (Aug 2026 rev. 6)
Annex A: A.8.15 Logging (Implemented) · A.8.16 Monitoring (Implemented – not a 24x7 outsourced SOC)
```

FluxeHra ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SIEM-AXIOM — Axiom security SIEM monitors (screenshot)

EV-SUPPLIER-VERCEL — Vercel supplier assurance summary

- **Show:** Sanitized evidence card: certificate/attestation on file (Jul 2026) — no account secrets
- **Test:** Annual re-review; align with Trust Center hosting regions
- **Code / config:** Provider file (private); `vercel.json` region `dub1`

EV-SUPPLIER-VERCEL

Sanitized — no nominative PII

Vercel supplier assurance

Supplier: Vercel Inc. (application hosting / Edge)  
Evidence on file (private): supplier certificate / attestation - dated 28 Jul 2026  
Product alignment: `vercel.json` region `dub1` (Dublin)  
Customer-facing note: see Trust Center /trust - Hosting & sub-processors  
Cadence: re-review annually; watch `status.vercel.com` for changes  
Annex A: A.5.19 / A.5.21 / A.5.22 Implemented · A.5.20 Partial (customer DPA)

FluxeHra ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SUPPLIER-VERCEL — Vercel supplier assurance summary (screenshot)

EV-SUPPLIER-SUPABASE — Supabase supplier assurance summary

- **Show:** Sanitized evidence card: certificate/attestation on file (Jul 2026) — region eu-west-1
- **Test:** Annual re-review; document backup plan RPO/RTO in Provider ISMS
- **Code / config:** Provider file (private); Trust Center hosting section

EV-SUPPLIER-SUPABASE

Sanitized — no nominative PII

Supabase supplier assurance

Supplier: Supabase (PostgreSQL, Auth, Storage)  
Evidence on file (private): supplier certificate / attestation - dated 28 Jul 2026  
Production region documented: eu-west-1 (Ireland)  
Backup / RPO-RTO: document targets in Provider ISMS from Supabase plan  
Annex A: A.5.19 / A.5.21 / A.5.22 / A.5.30 Implemented · A.5.20 Partial (customer DPA)

FluxeHRa ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SUPPLIER-SUPABASE — Supabase supplier assurance summary (screenshot)

EV-SUPPLIER-CURS0R — Cursor / Anysphere supplier assurance summary

- **Show:** Sanitized card: SOC 2 Type II + security program / NDA on file for development tooling
- **Test:** Does not replace FluxeHRa pen-test; keep tool assurance separate from product SoA
- **Code / config:** Provider file (private)

EV-SUPPLIER-CURS0R

Sanitized — no nominative PII

Cursor / Anysphere tooling assurance

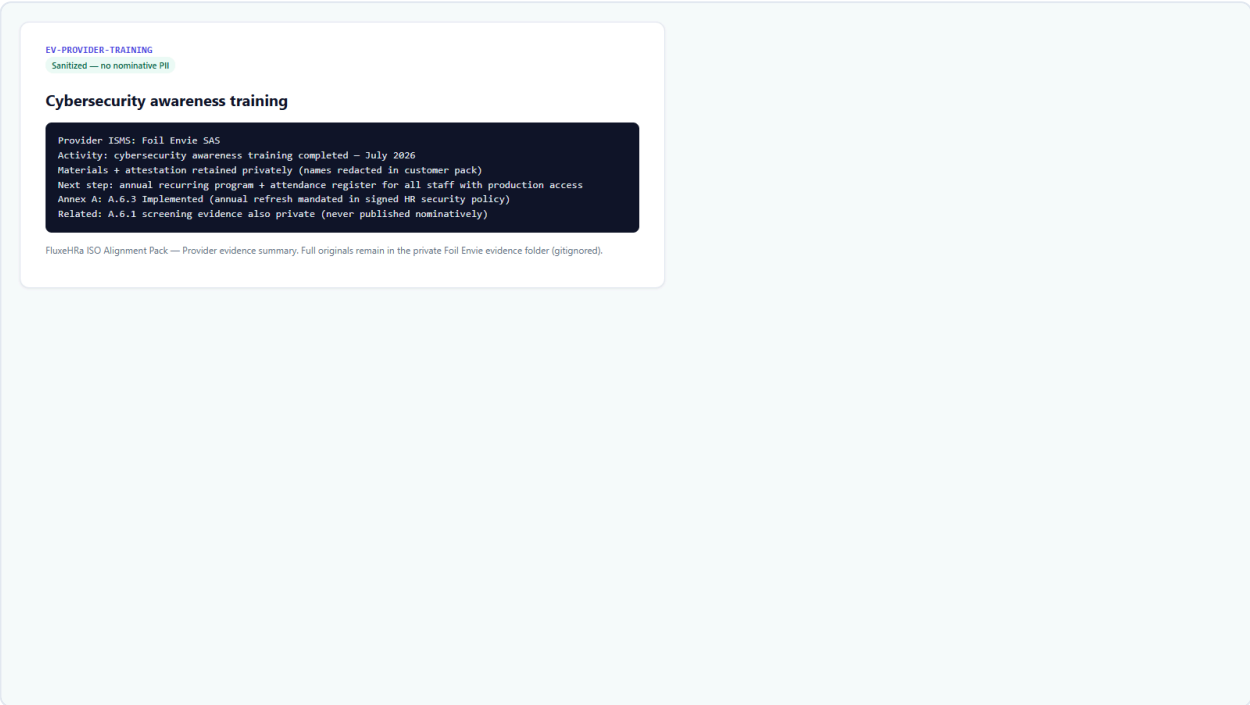
Supplier: Anysphere (Cursor) — development tooling (not a FluxeHRa runtime sub-processor for HR PII)  
Evidence on file (private): SOC 2 Type II (2025), security program update, pen-test executive summary, NDA  
Scope note: tool assurance ≠ FluxeHRa product pen-test or ISO certificate  
Annex A: A.5.19 / A.5.21 / A.6.6 Implemented · A.5.35 Partial (Independent FluxeHRa ISMS review)

FluxeHRa ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SUPPLIER-CURS0R — Cursor / Anysphere supplier assurance summary (screenshot)

EV-PROVIDER-TRAINING — Cybersecurity awareness training (Provider)

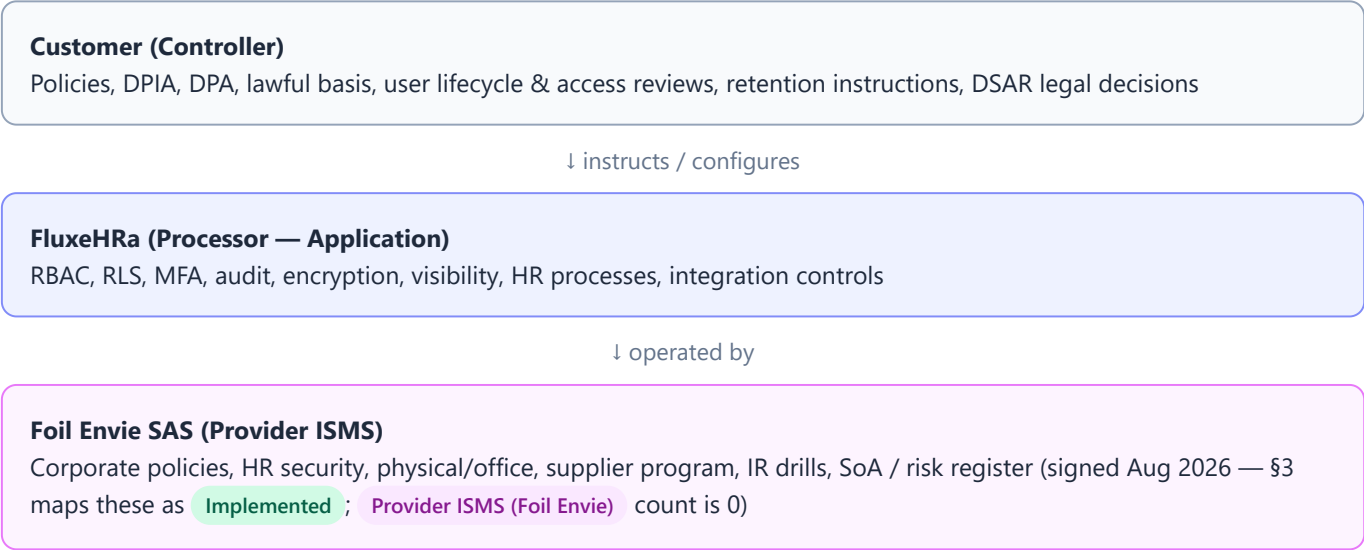
- **Show:** Sanitized card: training completed Jul 2026 — no personal names in customer pack
- **Test:** Retain full attestation privately; extend to annual all-staff program
- **Code / config:** Provider ISMS (private folder)



EV-PROVIDER-TRAINING — Cybersecurity awareness training (Provider) (screenshot)

[↑ Table of contents](#) · [↑ Languages](#)

11. Shared responsibility model (ISO 27017)



↓ runs on

### Sub-processors

Supabase (PostgreSQL, Auth, Storage — eu-west-1) · Vercel (app/API — dub1) · Axiom (security SIEM — US East edge)

Customers should record sub-processor regions and contracts in their processing register. Foil Envie ISMS artefacts for solo-operator scope are signed (August 2026); legal ISO/SOC *certification* remains an external engagement (A.5.35).

[↑ Table of contents](#) · [↑ Languages](#)

## 12. Recommendations — more auditable & customer-reassuring

1. **Signed customer DPA** (A.5.20 / A.5.31) — legal finalize of `public/legal/dpa*.md` with the first commercial customer (track already signed).
2. **Independent ISMS review** (A.5.35) — external audit or ISO certification campaign when budgeted.
3. **Restore drill** — within 30 days of Supabase Pro activation (A.5.30 already Implemented with commitment).
4. **Optional:** Sentry APM; live browser E2E IDOR against a demo org; set `PRODUCTION_SUPABASE_URL` on Vercel Preview/Dev to harden the non-prod URL guard.

[↑ Table of contents](#) · [↑ Languages](#)

## 13. Known gaps (honest summary)

- No ISO / SOC *certificate* claimed by the product (company certification remains external).
- Provider ISMS artefacts (Jul–Aug 2026): supplier certificates, training, screening, **signed** IR/Backup/NDA Wave A/B, plus **signed** maximize pack (2026-08-13): ISMS-governance, acceptable use, classification/cloud, staff secrets, home-office physical, people lifecycle, duty-to-report/evidence, records retention, asset/config/source, endpoint attestation, audit-testing/IP, Secure-development-pack — private under `Certification documentation/`. Annex A refreshed to Implemented where evidence is complete.
- Few Annex A rows remain open: A.5.20 / A.5.31 (customer DPA), A.5.35 (independent review). A.5.6 closed — see `EV-SECURITY-WATCH` (Security Watch + signed subscriptions). A.8.23 closed (web-filter N/A + compensating).
- Retention analyze/purge is implemented server-side (no longer UI theatre).
- DSAR portable export + in-place anonymization available to HR/Admin (legal-hold aware).
- MFA for privileged roles (admin / super\_admin / hr / Domain Admin) defaults **ON** in production.
- Core HR hire / update / terminate emit audit events.
- Password set/reset UI and welcome/reset emails display the  $\geq 20$  + complexity rule; existing passwords keep working until changed.
- Trust Center at `/trust`; vulnerability contact `contact@fluxehra.ai`; `SECURITY.md`, IR, backup/restore, sub-processors, AIPD support pack shipped.
- Compliance evidence JSON export; `npm run test:security-smoke`, `test:security-idor`, GitHub `security-tests` workflow.
- Remaining honest gaps: optional Sentry APM; **customer DPA** (A.5.20/A.5.31); **independent review** (A.5.35); restore drill after Supabase Pro. A.5.6 closed via `EV-SECURITY-WATCH`. A.8.23 closed via web-filter N/A compensating controls.
- Authenticated UI evidence screens may still show placeholders until a disposable demo org session is captured — see `docs/iso-demo-session-capture-guide.md`.

This pack reflects application state at generation time. Questions: `contact@fluxehra.ai`



# Pack d'alignement normes ISO (clients)

FluxeHRa / Flex HR — Alignement & préparation des contrôles (pas une certification)

Destinataires : IT, RSSI, DPO, achats, auditeurs clients

Version document : septembre 2026 (rév. 21) — e-signature FluxeHRa : standards eIDAS SES + PAdES-B optionnel

## Sommaire

1. 1. Positionnement & lecture du pack
2. 2. ISO/IEC 27001 — Management de la sécurité de l'information
3. 3. ISO/IEC 27001:2022 Annexe A — catalogue complet des contrôles
4. 4. ISO/IEC 27017 — Sécurité des services cloud
5. 5. ISO/IEC 27018 — Protection des PII dans le cloud public
6. 6. ISO/IEC 27701 — Management de la protection de la vie privée
7. 7. ISO/IEC 25010 — Qualité du produit logiciel
8. 8. Matrice de contrôles (vue thématique compacte)
9. 9. Catalogue des processus de bout en bout
10. 10. Pack de preuves — comment démontrer
11. 11. Modèle de responsabilité partagée (ISO 27017)
12. 12. Recommandations — plus auditable & rassurant
13. 13. Écarts connus (synthèse honnête)

## 1. Positionnement & lecture du pack

**FluxeHRa n'est pas certifié ISO à ce jour.** Ce pack cartographie les contrôles techniques produit *et* le catalogue complet de l'annexe A ISO/IEC 27001:2022 (gouvernance, RH, physique inclus) pour donner aux clients une vue de *toutes* les dimensions — y compris hors code. Il sert à la due diligence IT, pas de substitut à un audit de certification SMSI.

Légende des statuts :

- **Implémenté** — contrôle implémenté et démontrable.
- **Partiel** — présent mais incomplet.
- **Plateforme / sous-traitant** — principalement fourni par Supabase / Vercel ; à documenter contractuellement.
- **Responsabilité client** — responsabilité organisationnelle du client (responsable de traitement).
- **SMSI éditeur (Foil Envie)** — SMSI organisationnel Foil Envie SAS (politiques, sécurité RH, locaux, programme fournisseurs, exercices IR) — feuille de route éditeur, indépendante des features applicatives.
- **Écart / feuille de route** — écart connu ; voir feuille de route (§12).

Document compagnon : [Livre blanc sécurité & conformité](#). Production : <https://fluxehra.ai>.

Check-list interne de captures : `docs/iso-evidence-capture-checklist.md`. Guide session démo : `docs/iso-demo-session-capture-guide.md`. Playbook gaps : `docs/iso-gap-priority-playbook.md`. Preuves nominatives Provider hors public/.

## 2. ISO/IEC 27001 — Management de la sécurité de l'information

**Attentes clés** : un SMSI fondé sur les risques (politiques, accès, crypto, exploitation, journalisation, fournisseurs, sécurité des personnes, sécurité physique, amélioration continue). L'annexe A (2022) catalogue **93 contrôles** ; la certification audit *l'organisation* (Foil Envie en tant que sous-traitant + le client en tant que responsable), pas seulement le logiciel.

**Position FluxeHRa** : contrôles techniques solides pour un SIRH multi-tenant. Le SMSI Foil Envie (opérateur unique) est **signé** (août 2026) et cartographié **Implémenté** au §3. Les devoirs du responsable de traitement restent côté client.

**Forces** : API refus par défaut, RLS, chiffrement, MFA, audit (proxy), CSP/HSTS/rate limits/SSRF, pack SMSI signé, SIEM Axiom, backups documentés.

**Ouverts Annexe A** : DPA client (A.5.20 / A.5.31) ; revue indépendante (A.5.35). A.5.6 clos (Security Watch + abonnements signés 2026-08-14). Les lignes **Plateforme / sous-traitant** sont des datacenters cloud, pas du travail produit inachevé. Optionnel : APM Sentry ; restore drill après Pro.

**Le client doit encore** : tenir son SMSI ; revues d'accès ; DPA ; MFA/Turnstile ; superviser l'audit ; utiliser le pack support AIPD.

## 3. ISO/IEC 27001:2022 Annexe A — catalogue complet des contrôles

Catalogue complet de l'**annexe A ISO/IEC 27001:2022** (93 contrôles). Le SMSI Foil Envie (opérateur unique) est largement documenté et signé (août 2026) : la plupart des lignes organisationnelles / RH / physiques sont **Implémenté**. Restent ouverts : DPA client (A.5.20 / A.5.31), revue indépendante (A.5.35). Les lignes **Plateforme / sous-traitant** sont des datacenters cloud (Supabase / Vercel), pas des écarts produit.

### Comment lire les colonnes statut et ownership

- **Implémenté** — démontrable dans le produit FluxeHRa.
- **Partiel** — partiellement couvert (produit et/ou processus).
- **Plateforme / sous-traitant** — surtout Supabase / Vercel.
- **Responsabilité client** — responsabilité du client (responsable de traitement).
- **SMSI éditeur (Foil Envie)** — SMSI organisationnel Foil Envie encore ouvert (aucun à ce jour ; A.5.6 clos).
- **Écart / feuille de route** — écart produit / processus à traiter.
- **App** — entièrement démontrable dans le produit / CI FluxeHRa.
- **Entreprise (politique)** — SMSI Foil Envie (RH, juridique, physique, audit externe).
- **Mixte** — tranche produit + artefacts Entreprise (et parfois Client) encore requis.

### Répartition actuelle des statuts

- **Implémenté** — 77
- **Partiel** — 3
- **Plateforme / sous-traitant** — 13
- **Responsabilité client** — 0
- **SMSI éditeur (Foil Envie)** — 0
- **Écart / feuille de route** — 0

### Répartition par ownership (qui peut clôturer le contrôle)

- **App — 12**
- **Entreprise (politique) — 40**
- **Mixte — 41**

| ID    | Intitulé du contrôle                                | Thème                            | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                                                                                                                                                          | Statut     |
|-------|-----------------------------------------------------|----------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| A.5.1 | Politiques de sécurité de l'information             | A.5 — Contrôles organisationnels | Entreprise (politique) | Politique SMSI cadre (Certification documentation/policies/ISMS-governance (PDF privé signé 2026-08-13)) — opérateur unique Foil Envie août 2026.                                                                                                                                                                                                   | Implémenté |
| A.5.2 | Rôles et responsabilités en matière de sécurité     | A.5 — Contrôles organisationnels | Entreprise (politique) | Responsables sécurité & privacy nommés (Irwin Rouch) dans ISMS-governance (PDF privé signé 2026-08-13) ; RBAC produit pour les rôles app.                                                                                                                                                                                                           | Implémenté |
| A.5.3 | Séparation des tâches                               | A.5 — Contrôles organisationnels | Mixte                  | Produit : SU / org admin / HR ; grant SU 48 h Org Admin. Break-glass solo signé août 2026 (Certification documentation/ops/Break-glass-solo) ; double contrôle prévu à l'embauche #2.                                                                                                                                                               | Implémenté |
| A.5.4 | Responsabilités de la direction                     | A.5 — Contrôles organisationnels | Entreprise (politique) | Engagement direction & ressources documentés dans ISMS-governance (PDF privé signé 2026-08-13) (Axiom, MFA, backups Pro, IR, revue d'accès).                                                                                                                                                                                                        | Implémenté |
| A.5.5 | Contact avec les autorités                          | A.5 — Contrôles organisationnels | Entreprise (politique) | Processus contact CNIL / autorités dans ISMS-governance (PDF privé signé 2026-08-13) §4 ; le client reste responsable de traitement.                                                                                                                                                                                                                | Implémenté |
| A.5.6 | Contact avec des groupes d'intérêt spéciaux         | A.5 — Contrôles organisationnels | Entreprise (politique) | Contact CERT-FR / CISA / OSV via SU Admin Security Watch (RSS + lockfile, filtré impact) + Action GitHub quotidienne + Dependabot. Registre d'abonnements signé 2026-08-14 (Certification documentation/policies/Security-community-subscriptions). Sauvegardes e-mail : avis CERT-FR, CISA KEV, statuts vendors. Pas d'ISAC payant (proportionné). | Implémenté |
| A.5.7 | Veille sur les menaces                              | A.5 — Contrôles organisationnels | Entreprise (politique) | Veille : SU Admin Security Watch (OSV/KEV/CERT-FR, filtré impact) + Dependabot + Components Update + statuts vendors + Axiom VULN_WATCH (Asset-config-source-privileges PDF privé signé 2026-08-13).                                                                                                                                                | Implémenté |
| A.5.8 | Sécurité de l'information dans la gestion de projet | A.5 — Contrôles organisationnels | Entreprise (politique) | Jalons sécurité projet dans Secure-development-pack (PDF privé signé 2026-08-13) (migrations, typecheck, smoke, secrets, SSRF).                                                                                                                                                                                                                     | Implémenté |

| ID     | Intitulé du contrôle                                        | Thème                            | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                               | Statut     |
|--------|-------------------------------------------------------------|----------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| A.5.9  | Inventaire des informations et autres actifs associés       | A.5 — Contrôles organisationnels | Entreprise (politique) | Inventaire actifs Foil Envie (GitHub, Vercel, Supabase, Axiom, domaine, laptop) dans Asset-config-source-privileges (PDF privé signé 2026-08-13) ; le client inventorie ses données org.                                 | Implémenté |
| A.5.10 | Usage acceptable des informations et autres actifs associés | A.5 — Contrôles organisationnels | Entreprise (politique) | Charte d'usage staff (Acceptable-use-remote-clear-desk (PDF privé signé 2026-08-13)) ; CGU produit pour les utilisateurs.                                                                                                | Implémenté |
| A.5.11 | Restitution des actifs                                      | A.5 — Contrôles organisationnels | Entreprise (politique) | Check-list sortie & restitution dans People-lifecycle (PDF privé signé 2026-08-13) ; produit : suppression org / restitution selon DPA.                                                                                  | Implémenté |
| A.5.12 | Classification de l'information                             | A.5 — Contrôles organisationnels | Mixte                  | Produit sensitive + visibilité ; schéma Public/Interne/Confidentiel/Restreint dans Classification-transfer-cloud (PDF privé signé 2026-08-13) aligné ENC2.                                                               | Implémenté |
| A.5.13 | Étiquetage de l'information                                 | A.5 — Contrôles organisationnels | Entreprise (politique) | Règles d'étiquetage docs/tickets Foil Envie dans Classification-transfer-cloud (PDF privé signé 2026-08-13) (même schéma que A.5.12).                                                                                    | Implémenté |
| A.5.14 | Transfert d'information                                     | A.5 — Contrôles organisationnels | Mixte                  | Produit TLS/exports/SSRF ; règles e-mail/USB/papier staff dans Classification-transfer-cloud (PDF privé signé 2026-08-13).                                                                                               | Implémenté |
| A.5.15 | Contrôle d'accès                                            | A.5 — Contrôles organisationnels | App                    | RBAC produit, RLS, MFA rôles privilégiés, API refus par défaut ; entrée org SU conditionnée à un grant client 48 h + RLS has_active_su_org_grant.                                                                        | Implémenté |
| A.5.16 | Gestion des identités                                       | A.5 — Contrôles organisationnels | App                    | Identities Supabase Auth ; SSO OIDC org ; invitations / reset.                                                                                                                                                           | Implémenté |
| A.5.17 | Informations d'authentification                             | A.5 — Contrôles organisationnels | Mixte                  | Produit mot de passe ≥20 + MFA TOTP ; coffre / MFA staff dans Staff-auth-secrets (PDF privé signé 2026-08-13). Console privée : Supabase Auth Multi-Factor TOTP Enabled (ops/Supabase-mfa-totp-enabled-2026-08-16.jpeg). | Implémenté |
| A.5.18 | Droits d'accès                                              | A.5 — Contrôles organisationnels | Mixte                  | Produit : Manage Roles, modules ; grants SU temporaires avec accept/refus Org Admin. Checklist revue d'accès signée août 2026 (Certification documentation/ops/Access-review-checklist) ; jeu trimestriel.               | Implémenté |

| ID     | Intitulé du contrôle                                                 | Thème                            | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                                                                              | Statut     |
|--------|----------------------------------------------------------------------|----------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| A.5.19 | Sécurité de l'information dans les relations avec les fournisseurs   | A.5 — Contrôles organisationnels | Entreprise (politique) | Registre TIC fournisseurs privé (Vercel, Supabase, Axiom, Cursor, DocuSign si utilisé) + cadence annuelle — Certification documentation/suppliers/Supplier-register.pdf ; PDF certs en privé. L'e-signature native FluxeHRA n'est pas un fournisseur séparé.            | Implémenté |
| A.5.20 | Prise en compte de la sécurité dans les accords fournisseurs         | A.5 — Contrôles organisationnels | Entreprise (politique) | DPA / trust docs sous-traitants collectés. DPA client bloqué jusqu'au premier client commercial (templates + DPA-signature-track signé) ; autres docs ops Wave A/B signés août 2026.                                                                                    | Partiel    |
| A.5.21 | Gestion de la sécurité dans la chaîne d'approvisionnement TIC        | A.5 — Contrôles organisationnels | Entreprise (politique) | Chaîne TIC couverte par Supplier-register (calendrier annuel + risques) ; suivi via status pages fournisseurs et Components Update.                                                                                                                                     | Implémenté |
| A.5.22 | Suivi, revue et gestion des changements des services fournisseurs    | A.5 — Contrôles organisationnels | Entreprise (politique) | Colonne prochaine revue + abonnements status pages dans Supplier-register ; revue annuelle selon calendrier privé.                                                                                                                                                      | Implémenté |
| A.5.23 | Sécurité de l'information pour l'utilisation des services cloud      | A.5 — Contrôles organisationnels | Mixte                  | Cloud approuvés (Supabase eu-west-1, Vercel dub1, Axiom) + préférence UE dans Classification-transfer-cloud (PDF privé signé 2026-08-13). Console privée : Vercel dub1 + Supabase prod FluxeHRA West EU / eu-west-1 (ops/Supabase-prod-general-region-2026-08-16.jpeg). | Implémenté |
| A.5.24 | Planification et préparation de la gestion des incidents de sécurité | A.5 — Contrôles organisationnels | Mixte                  | docs/incident-response.md + pack IR solo signé (août 2026) : RACI, tabletop 2026-08-11, accusé, capture moniteurs Axiom — privé Certification documentation/incident-response/.                                                                                         | Implémenté |
| A.5.25 | Évaluation et décision concernant les événements de sécurité         | A.5 — Contrôles organisationnels | Mixte                  | Matrice de sévérité dans docs/incident-response.md ; RACI opérateur unique (Irwin Rouch) signé en privé (août 2026).                                                                                                                                                    | Implémenté |
| A.5.26 | Réponse aux incidents de sécurité de l'information                   | A.5 — Contrôles organisationnels | Mixte                  | Produit : bug report / ops / Axiom. Exécution IR attestée via tabletop solo + accusé signés (août 2026, preuves privées).                                                                                                                                               | Implémenté |
| A.5.27 | Apprentissage à partir des incidents de sécurité                     | A.5 — Contrôles organisationnels | Mixte                  | Post-mortem dans la trame IR ; écarts/suivis du tabletop signé au dossier ; rejeu annuel prévu ; test:security-idor pour régressions.                                                                                                                                   | Implémenté |

| ID     | Intitulé du contrôle                                    | Thème                            | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                                                                                             | Statut                     |
|--------|---------------------------------------------------------|----------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.5.28 | Collecte des preuves                                    | A.5 — Contrôles organisationnels | Mixte                  | Journaux d'audit + export preuves ; playbook forensique dans Duty-to-report-and-evidence (PDF privé signé 2026-08-13).                                                                                                                                                                 | Implémenté                 |
| A.5.29 | Sécurité de l'information pendant une perturbation      | A.5 — Contrôles organisationnels | Mixte                  | Continuité via forfaits Supabase/Vercel + accusé Backup / pack IR signés (A.5.30). Pas un écart produit.                                                                                                                                                                               | Plateforme / sous-traitant |
| A.5.30 | Préparation des TIC pour la continuité d'activité       | A.5 — Contrôles organisationnels | Mixte                  | Engagement production documenté + accusé Backup signé (août 2026) : backups quotidiens Supabase Pro, rétention 7 j, RPO ≤ 24 h, RTO interne ≤ 4 h (docs/backup-restore.md) ; Pro + capture console Backups au premier client payant ; exercice restore sous 30 j après activation Pro. | Implémenté                 |
| A.5.31 | Exigences légales, réglementaires et contractuelles     | A.5 — Contrôles organisationnels | Mixte                  | Packs DPA/légaux livrés. Bloqué sur : DPA client signé + registre légal / revue conseil (Provider + Customer).                                                                                                                                                                         | Partiel                    |
| A.5.32 | Droits de propriété intellectuelle                      | A.5 — Contrôles organisationnels | Entreprise (politique) | Note PI / licences Foil Envie & OSS dans Audit-testing-IP-outsourcing (PDF privé signé 2026-08-13).                                                                                                                                                                                    | Implémenté                 |
| A.5.33 | Protection des enregistrements                          | A.5 — Contrôles organisationnels | Mixte                  | Rétention/purge produit + calendrier archivage corporate dans Records-retention-schedule (PDF privé signé 2026-08-13).                                                                                                                                                                 | Implémenté                 |
| A.5.34 | Vie privée et protection des PII                        | A.5 — Contrôles organisationnels | Mixte                  | Privacy produit : field_consent ESS, My preferences, DSAR, ENC2, redact PII fuites ; registre Art.30 docs/registre-activites-traitement-sous-traitant.md. PIMS / AIPD responsable = Customer + conseil Provider.                                                                       | Implémenté                 |
| A.5.35 | Revue indépendante de la sécurité de l'information      | A.5 — Contrôles organisationnels | Entreprise (politique) | Assurance tierce collectée pour outils clés (ex. Cursor SOC 2). Bloqué sur : revue indépendante FluxeHRA / SMSI Foil Envie (audit externe ou campagne ISO).                                                                                                                            | Partiel                    |
| A.5.36 | Conformité aux politiques, règles et normes de sécurité | A.5 — Contrôles organisationnels | Entreprise (politique) | Auto-revue trimestrielle définie dans ISMS-governance (PDF privé signé 2026-08-13) §5 (accès, vulnérabilités, fournisseurs, IR).                                                                                                                                                       | Implémenté                 |

| ID     | Intitulé du contrôle                                   | Thème                                     | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                                 | Statut                     |
|--------|--------------------------------------------------------|-------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.5.37 | Procédures d'exploitation documentées                  | A.5 — Contrôles organisationnels          | Entreprise (politique) | Procédures ops : docs/ (IR, backup-restore, SIEM, sous-traitants) + pack signé Certification documentation/ops (break-glass, revue d'accès, vulnérabilités, non-prod, suivi DPA) et accusés IR/backup.                     | Implémenté                 |
| A.6.1  | Vérification des antécédents                           | A.6 — Contrôles portant sur les personnes | Entreprise (politique) | Preuve de screening au dossier + politique RH sécurité signée août 2026 (Certification documentation/hr-security/) ; étendre à chaque embauche.                                                                            | Implémenté                 |
| A.6.2  | Modalités et conditions d'emploi                       | A.6 — Contrôles portant sur les personnes | Entreprise (politique) | Confidentialité contrat + NDA + accusé SMSI (People-lifecycle (PDF privé signé 2026-08-13)) ; NDA signé au dossier.                                                                                                        | Implémenté                 |
| A.6.3  | Sensibilisation, éducation et formation à la sécurité  | A.6 — Contrôles portant sur les personnes | Entreprise (politique) | Formation réalisée ; politique RH sécurité (signée août 2026) impose un rappel annuel pour le personnel à accès systèmes.                                                                                                  | Implémenté                 |
| A.6.4  | Processus disciplinaire                                | A.6 — Contrôles portant sur les personnes | Entreprise (politique) | Processus disciplinaire sécurité documenté dans People-lifecycle (PDF privé signé 2026-08-13).                                                                                                                             | Implémenté                 |
| A.6.5  | Responsabilités après cessation ou changement d'emploi | A.6 — Contrôles portant sur les personnes | Entreprise (politique) | Check-list de sortie (révoquer GitHub/Vercel/Supabase/Axiom, restituer, rappeler NDA) dans People-lifecycle (PDF privé signé 2026-08-13).                                                                                  | Implémenté                 |
| A.6.6  | Accords de confidentialité ou de non-divulgateion      | A.6 — Contrôles portant sur les personnes | Entreprise (politique) | NDA partenaire/outil au dossier (ex. Anysphere/Cursor). NDA salarié signé pour l'opérateur unique Irwin Rouch (août 2026) — privé Certification documentation/hr-security/ ; modèle réutilisable pour futurs recrutements. | Implémenté                 |
| A.6.7  | Travail à distance                                     | A.6 — Contrôles portant sur les personnes | Entreprise (politique) | Règles télétravail (chiffrement disque, verrouillage, pas de Wi-Fi ouvert pour admin prod) dans Acceptable-use-remote-clear-desk (PDF privé signé 2026-08-13).                                                             | Implémenté                 |
| A.6.8  | Notification des événements de sécurité                | A.6 — Contrôles portant sur les personnes | Mixte                  | Bug report in-app + devoir de signalement staff dans Duty-to-report-and-evidence (PDF privé signé 2026-08-13).                                                                                                             | Implémenté                 |
| A.7.1  | Périmètres de sécurité physique                        | A.7 — Contrôles physiques                 | Mixte                  | Datacenters = cloud Supabase/Vercel. Périmètre home-office Foil Envie couvert par A.7.3 (Home-office-physical-media signé).                                                                                                | Plateforme / sous-traitant |

| ID     | Intitulé du contrôle                                         | Thème                     | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                              | Statut                     |
|--------|--------------------------------------------------------------|---------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.7.2  | Contrôle d'accès physique                                    | A.7 — Contrôles physiques | Mixte                  | Contrôles d'entrée datacenter cloud. Visiteurs home-office Foil Envie sous A.7.6 (signé).                                                                               | Plateforme / sous-traitant |
| A.7.3  | Sécurisation des bureaux, salles et installations            | A.7 — Contrôles physiques | Entreprise (politique) | Contrôles physiques home-office (logement verrouillable, pas d'impressions Restreintes sans surveillance) dans Home-office-physical-media (PDF privé signé 2026-08-13). | Implémenté                 |
| A.7.4  | Surveillance de la sécurité physique                         | A.7 — Contrôles physiques | Mixte                  | Surveillance DC via cloud. Home-office : pas de CCTV DC ; verrouillage logement sous A.7.3.                                                                             | Plateforme / sous-traitant |
| A.7.5  | Protection contre les menaces physiques et environnementales | A.7 — Contrôles physiques | Mixte                  | Résilience régions cloud. Environnement home-office couvert par Home-office-physical-media (signé).                                                                     | Plateforme / sous-traitant |
| A.7.6  | Travail dans des zones sécurisées                            | A.7 — Contrôles physiques | Entreprise (politique) | Règles visiteurs / zone de travail home-office dans Home-office-physical-media (PDF privé signé 2026-08-13) (pas de site multi-employés dédié).                         | Implémenté                 |
| A.7.7  | Bureau et écran dégagés                                      | A.7 — Contrôles physiques | Entreprise (politique) | Bureau / écran dégagés dans Acceptable-use-remote-clear-desk (PDF privé signé 2026-08-13).                                                                              | Implémenté                 |
| A.7.8  | Emplacement et protection des équipements                    | A.7 — Contrôles physiques | Entreprise (politique) | Placement équipement laptop opérateur ; hardware cloud = Platform — Home-office-physical-media (PDF privé signé 2026-08-13).                                            | Implémenté                 |
| A.7.9  | Sécurité des actifs hors site                                | A.7 — Contrôles physiques | Entreprise (politique) | Règles hors site laptop (chiffrement, minimiser PII locales) dans Home-office-physical-media (PDF privé signé 2026-08-13).                                              | Implémenté                 |
| A.7.10 | Supports de stockage                                         | A.7 — Contrôles physiques | Entreprise (politique) | Supports amovibles (préférer cloud ; chiffrer si USB) dans Home-office-physical-media (PDF privé signé 2026-08-13).                                                     | Implémenté                 |
| A.7.11 | Services généraux de support                                 | A.7 — Contrôles physiques | Mixte                  | Énergie/froid datacenters cloud. Pas d'utilités de site dédié Foil Envie (home-office / cloud).                                                                         | Plateforme / sous-traitant |
| A.7.12 | Sécurité du câblage                                          | A.7 — Contrôles physiques | Mixte                  | Câblage DC cloud. Pas de salle comms dédiée Foil Envie (home-office / cloud).                                                                                           | Plateforme / sous-traitant |
| A.7.13 | Maintenance des équipements                                  | A.7 — Contrôles physiques | Mixte                  | Maintenance matérielle cloud. Effacement laptop opérateur sous A.7.14 (signé).                                                                                          | Plateforme / sous-traitant |
| A.7.14 | Mise au rebut ou réutilisation                               | A.7 — Contrôles physiques | Entreprise (politique) | Effacement / destruction sécurisée des appareils Foil Envie ; cloud =                                                                                                   | Implémenté                 |

| ID     | Intitulé du contrôle                         | Thème                          | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                                                                                                            | Statut                     |
|--------|----------------------------------------------|--------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
|        | sécurisée des équipements                    |                                |                        | Platform — Home-office-physical-media (PDF privé signé 2026-08-13).                                                                                                                                                                                                                                   |                            |
| A.8.1  | Terminaux utilisateurs                       | A.8 — Contrôles technologiques | Entreprise (politique) | Chiffrement / durcissement endpoint opérateur attesté dans Endpoint-malware-attestation (PDF privé signé 2026-08-13) (appareils clients = Customer).                                                                                                                                                  | Implémenté                 |
| A.8.2  | Droits d'accès privilégiés                   | A.8 — Contrôles technologiques | App                    | Isolation plateforme SU Admin ; données tenant seulement avec grant Org Admin 48 h ; MFA aal2 pour admin / super_admin / HR / Domain Admin ; proxy audité après entrée ; service_role serveur uniquement.                                                                                             | Implémenté                 |
| A.8.3  | Restriction d'accès à l'information          | A.8 — Contrôles technologiques | App                    | RLS, visibilité champs, accès documents, assert périmètre org.                                                                                                                                                                                                                                        | Implémenté                 |
| A.8.4  | Accès au code source                         | A.8 — Contrôles technologiques | Entreprise (politique) | Repo GitHub privé + moindre privilège documentés dans Asset-config-source-privileges (PDF privé signé 2026-08-13).                                                                                                                                                                                    | Implémenté                 |
| A.8.5  | Authentification sécurisée                   | A.8 — Contrôles technologiques | App                    | PKCE, politique mot de passe ≥20 avec majuscule, minuscule, chiffre et caractère spécial, MFA TOTP pour admin / super_admin / HR / Domain Admin (défaut ON en production), Turnstile optionnel, OIDC org. Console privée : Supabase MFA TOTP Enabled (ops/Supabase-mfa-totp-enabled-2026-08-16.jpeg). | Implémenté                 |
| A.8.6  | Gestion de la capacité                       | A.8 — Contrôles technologiques | Mixte                  | Capacité élastique Vercel/Supabase ; Components Update + moniteurs Axiom pour signaux de charge.                                                                                                                                                                                                      | Plateforme / sous-traitant |
| A.8.7  | Protection contre les logiciels malveillants | A.8 — Contrôles technologiques | Entreprise (politique) | Attestation AV/Defender OS + limites zip SCORM produit — Endpoint-malware-attestation (PDF privé signé 2026-08-13).                                                                                                                                                                                   | Implémenté                 |
| A.8.8  | Gestion des vulnérabilités techniques        | A.8 — Contrôles technologiques | App                    | Components Update + Security Watch (OSV/KEV) + PRs Dependabot + CI `npm run audit:deps` (élevé/critique) avec waivers AUDIT_ALLOWLIST ; SLA Critique ≤7 j / Élevé ≤30 j affiché dans SU Admin.                                                                                                        | Implémenté                 |
| A.8.9  | Gestion de configuration                     | A.8 — Contrôles technologiques | Mixte                  | Baselines config (migrations, vercel.json, inventaire env) dans Asset-config-source-privileges (PDF privé signé 2026-08-13).                                                                                                                                                                          | Implémenté                 |
| A.8.10 | Suppression d'information                    | A.8 — Contrôles technologiques | App                    | Cascade suppression org, anonymisation DSAR, APIs de purge                                                                                                                                                                                                                                            | Implémenté                 |

| ID     | Intitulé du contrôle                                     | Thème                          | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                                                                                                               | Statut                     |
|--------|----------------------------------------------------------|--------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
|        |                                                          |                                |                        | rétenion.                                                                                                                                                                                                                                                                                                |                            |
| A.8.11 | Masquage des données                                     | A.8 — Contrôles technologiques | App                    | Chiffrement ENC2 au repos + déchiffrement selon rôle ; CSV/API/SFTP/DSAR autorisés restent en clair. Canaux de fuite (bug/erreur) : rédaction IBAN/SSN.                                                                                                                                                  | Implémenté                 |
| A.8.12 | Prévention des fuites de données                         | A.8 — Contrôles technologiques | Mixte                  | Baseline DLP produit : auth export, rate limits, storage privé, redact PII bugs, événements BULK_EXPORT. DLP CASB/endpoint entreprise non déployé (Customer/Provider optionnel).                                                                                                                         | Implémenté                 |
| A.8.13 | Sauvegarde de l'information                              | A.8 — Contrôles technologiques | Mixte                  | Backups quotidiens Supabase Pro (rétenion 7 j) engagés pour le premier client payant ; RPO ≤ 24 h et RTO interne ≤ 4 h dans docs/backup-restore.md et accusé Backup signé (août 2026) ; PITR optionnel ; objets Storage hors backup BDD (documenté). Capture UI Backups différée jusqu'à activation Pro. | Implémenté                 |
| A.8.14 | Redondance des installations de traitement               | A.8 — Contrôles technologiques | Mixte                  | Résilience multi-AZ cloud. RPO/RTO Foil Envie documentés (A.5.30). Pas de multi-région active-active revendiqué.                                                                                                                                                                                         | Plateforme / sous-traitant |
| A.8.15 | Journalisation                                           | A.8 — Contrôles technologiques | App                    | audit_logs (piste métier) + SIEM SECURITY_EVENT via Axiom (fluxehra_logs) ; télémétrie authz/tenant/RLS/échecs d'auth/cron/HMAC/SSRF sans PII (août 2026 rév. 6).                                                                                                                                        | Implémenté                 |
| A.8.16 | Activités de surveillance                                | A.8 — Contrôles technologiques | Mixte                  | Moniteurs Axiom (3 slots) actifs : BOLA/tenant, force brute par IP, high-signal (cron/RLS/HMAC/SSRF) ; preuve privée EV-SIEM-AXIOM-monitors.png (août 2026) ; Vercel Analytics + ops ; RACI IR solo pour la réponse. Pas un SOC 24x7 externalisé.                                                        | Implémenté                 |
| A.8.17 | Synchronisation des horloges                             | A.8 — Contrôles technologiques | Mixte                  | NTP cloud ; horodatage applicatif côté serveur.                                                                                                                                                                                                                                                          | Plateforme / sous-traitant |
| A.8.18 | Utilisation de programmes utilitaires privilégiés        | A.8 — Contrôles technologiques | Entreprise (politique) | Utilitaires prod DB/console réservés au Security Owner — Asset-config-source-privileges (PDF privé signé 2026-08-13) + Break-glass-solo.                                                                                                                                                                 | Implémenté                 |
| A.8.19 | Installation de logiciels sur les systèmes opérationnels | A.8 — Contrôles technologiques | Mixte                  | Déploiements prod uniquement via CI Vercel depuis le repo autorisé — Asset-config-source-privileges (PDF privé signé 2026-08-13).                                                                                                                                                                        | Implémenté                 |

| ID     | Intitulé du contrôle                                            | Thème                          | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                                                                                          | Statut                     |
|--------|-----------------------------------------------------------------|--------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.8.20 | Sécurité des réseaux                                            | A.8 — Contrôles technologiques | Mixte                  | Sécurité réseau cloud. Hygiène réseau télétravail sous Acceptable-use-remote-clear-desk (signé).                                                                                                                                                                                    | Plateforme / sous-traitant |
| A.8.21 | Sécurité des services réseau                                    | A.8 — Contrôles technologiques | App                    | HTTPS/HSTS ; garde SSRF sur webhooks, SFTP, OIDC token/JWKS, hôtes SMTP et URLs IdP authorize/SAML SSO (https + hôtes publics).                                                                                                                                                     | Implémenté                 |
| A.8.22 | Séparation des réseaux                                          | A.8 — Contrôles technologiques | Mixte                  | Isolation VPC cloud. Séparation prod/Dev Foil Envie : projets Vercel distincts (fluxehra.ai vs saas-flex-hr-sql-dev) + Supabase FluxeHRA-dev (eu-west-1) ; captures console privées sous Certification documentation/ops/ ; politique non-prod (signée) + assertNonProdSupabaseUrl. | Plateforme / sous-traitant |
| A.8.23 | Filtrage web                                                    | A.8 — Contrôles technologiques | Entreprise (politique) | N/A proxy web entreprise (pas de parc) ; compensations SmartScreen/Defender + hygiène DNS laptop opérateur — Certification documentation/policies/Web-filtering-NA-compensating. Réévaluer si parc staff grandit.                                                                   | Implémenté                 |
| A.8.24 | Utilisation de la cryptographie                                 | A.8 — Contrôles technologiques | App                    | TLS en transit ; AES-256-GCM champs ; clé privée DocuSign chiffrée au repos si ce moteur est utilisé ; jetons / OTP e-signature FluxeHRA stockés hachés uniquement.                                                                                                                 | Implémenté                 |
| A.8.25 | Cycle de vie de développement sécurisé                          | A.8 — Contrôles technologiques | Mixte                  | Politique SDLC sécurisé dans Secure-development-pack (PDF privé signé 2026-08-13) (migrations, typecheck, smoke, CSP).                                                                                                                                                              | Implémenté                 |
| A.8.26 | Exigences de sécurité des applications                          | A.8 — Contrôles technologiques | Mixte                  | Check-list exigences sécurité applicative dans Secure-development-pack (PDF privé signé 2026-08-13) (RLS, authz, secrets, SSRF, ENC2).                                                                                                                                              | Implémenté                 |
| A.8.27 | Principes d'architecture et d'ingénierie des systèmes sécurisés | A.8 — Contrôles technologiques | App                    | Navigateur non fiable ; authz serveur ; RLS ; défense en profondeur (livre blanc).                                                                                                                                                                                                  | Implémenté                 |
| A.8.28 | Codage sécurisé                                                 | A.8 — Contrôles technologiques | Mixte                  | Check-list coding sécurisé (escapeHtml/DOMPurify/path gateway/audit:deps) dans Secure-development-pack (PDF privé signé 2026-08-13).                                                                                                                                                | Implémenté                 |

| ID     | Intitulé du contrôle                                                     | Thème                          | Ownership              | Note FluxeHRA / Foil Envie                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Statut     |
|--------|--------------------------------------------------------------------------|--------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| A.8.29 | Tests de sécurité en développement et en recette                         | A.8 — Contrôles technologiques | Mixte                  | Gates d'acceptation : security-smoke, security-idor, audit:deps via workflow GitHub security-tests + Secure-development-pack (PDF privé signé 2026-08-13). Pentest externe reste un engagement futur.                                                                                                                                                                                                                                                                         | Implémenté |
| A.8.30 | Développement externalisé                                                | A.8 — Contrôles technologiques | Entreprise (politique) | Pas de développement externalisé actuellement ; règles contractors si engagement — Audit-testing-IP-outsourcing (PDF privé signé 2026-08-13).                                                                                                                                                                                                                                                                                                                                 | Implémenté |
| A.8.31 | Séparation des environnements de développement, de test et de production | A.8 — Contrôles technologiques | Mixte                  | Pistes dédiées (août 2026) : Git main → Vercel saas-flex-hr-sql + Supabase FluxeHRA (prod, eu-west-1) ; Git dev → Vercel saas-flex-hr-sql-dev + Supabase FluxeHRA-dev (eu-west-1). Preuves privées : ops/EV-ENV-SEPARATION-*-2026-08-16.png + captures console (domaines, dub1, noms d'env, Deployment Protection, région prod, URLs Auth) — docs/provider-isms-evidence.md. Politique non-prod signée ; assertNonProdSupabaseUrl si PRODUCTION_SUPABASE_URL sur Preview/Dev. | Implémenté |
| A.8.32 | Gestion des changements                                                  | A.8 — Contrôles technologiques | Mixte                  | Gestion du changement = Git + déploiement Vercel pour opérateur unique (Secure-development-pack (PDF privé signé 2026-08-13)) ; CAB reporté jusqu'à croissance d'équipe.                                                                                                                                                                                                                                                                                                      | Implémenté |
| A.8.33 | Informations de test                                                     | A.8 — Contrôles technologiques | Mixte                  | Outil dummy-data + politique non-prod signée août 2026 (pas de dumps prod ; redacter si copie exceptionnelle) — Certification documentation/ops/Non-prod-data-policy.                                                                                                                                                                                                                                                                                                         | Implémenté |
| A.8.34 | Protection des systèmes d'information lors des tests d'audit             | A.8 — Contrôles technologiques | Entreprise (politique) | Règles pour tests d'audit client/vendor vs production dans Audit-testing-IP-outsourcing (PDF privé signé 2026-08-13).                                                                                                                                                                                                                                                                                                                                                         | Implémenté |

Catalogue vivant de type DdA. Les lignes **Partiel** restantes sont A.5.20, A.5.31, A.5.35. **Plateforme / sous-traitant** = datacenters sous-traitants. **SMSI éditeur (Foil Envie)** = 0.

[↑ Sommaire](#) · [↑ Langues](#)

## 4. ISO/IEC 27017 — Sécurité des services cloud

**Attentes clés** : guidance cloud (responsabilité partagée, isolation, admin, journalisation cloud).

**Position FluxeHRa** : modèle §11 ; isolation RLS + périmètre API ; proxy sans élévation JWT ; SSO IdP client ; couche SMSI éditeur ( [SMSI éditeur \(Foil Envie\)](#) ).

**Forces** : RLS, chemins Storage org, HMAC/export par clé d'intégration, régions UE documentées, accès SU aux données client via grant 48 h (deploy config = gestion des changements distincte).

**Résiduel** : PRA/PCA datacenter = [Plateforme / sous-traitant](#) (Supabase/Vercel). DPA client = A.5.20 / A.5.31.

**Le client doit encore** : configurer SSO/rôles ; conserver preuves régionales et contrats sous-traitants.

[↑ Sommaire](#) · [↑ Langues](#)

---

## 5. ISO/IEC 27018 — Protection des PII dans le cloud public

**Attentes clés** : protection des données à caractère personnel chez un processeur cloud (finalité, transparence, restitution/effacement, sécurité).

**Position FluxeHRa** : chiffrement sensible, visibilité, DMS privé, hébergement UE, jetons d'embauche hachés ; pas d'usage secondaire publicitaire des PII RH.

**Résiduel** : consentement catégories particulières via `field_consent` + My preferences. Pas de *certificat* ISO/SOC (campagne externe = A.5.35).

**Le client doit encore** : base légale, DPIA, calendrier de conservation, procédures droits des personnes.

[↑ Sommaire](#) · [↑ Langues](#)

---

## 6. ISO/IEC 27701 — Management de la protection de la vie privée

**Attentes clés** : extension 27001 pour un PIMS (responsable vs sous-traitant).

**Position FluxeHRa** : typiquement **sous-traitant** ; le client est **responsable de traitement**. Mesures techniques PIMS livrées (visibilité, DSAR, rétention, consentements, registre Art.30, IR). DPIA / base légale / DPA client signé restent Customer (A.5.20 / A.5.31).

**Résiduel** : DPA client (premier client commercial) ; revue indépendante (A.5.35). Audit Core HR implémenté.

[↑ Sommaire](#) · [↑ Langues](#)

---

## 7. ISO/IEC 25010 — Qualité du produit logiciel

**Attentes clés** : modèle de qualité (adéquation fonctionnelle, performance, utilisabilité, fiabilité, sécurité, maintenabilité...).

**Position FluxeHRa** : Core HR bitemporel, performance, learning, compensation, analytics, intégrations — recrutement encore placeholder (seul Partial thématique 25010) ; sécurité en couches ; SIEM Axiom + Analytics Vercel. APM Sentry optionnel, non bloquant Annexe A.

[↑ Sommaire](#) · [↑ Langues](#)

---

## 8. Matrice de contrôles (vue thématique compacte)

Thèmes de synthèse (voir §3 pour le catalogue Annexe A complet). Les ID de preuve renvoient au §10.

| Thème                                        | Attente                                                                  | Implémentation FluxeHRa                                                                                                                                                             | Statut                     | Preuve                                                                          |
|----------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------------------------------------------------------------------------|
| Contrôle d'accès (27001 A.8)                 | Authentifier ; moindre privilège ; protéger les comptes privilégiés      | Supabase Auth (PKCE/JWT), RBAC ( <code>role_permissions</code> ), périmètre HR, MFA TOTP (défaut ON en production pour rôles privilégiés), idle timeout, API refus par défaut       | Implémenté                 | EV-AUTH-MFA, EV-RBAC-ROLES                                                      |
| Cryptographie (27001 A.8)                    | Protéger la confidentialité des données sensibles en transit et au repos | HTTPS/HSTS ; chiffrement AES-256-GCM ( <code>ENC2::</code> ) des champs <code>sensitive</code> ; clés d'intégration hachées                                                         | Implémenté                 | EV-CRYPTO-FIELD                                                                 |
| Journalisation (27001 A.8)                   | Enregistrer les événements de sécurité avec identité accountable         | <code>audit_logs</code> (réel vs proxy) ; UI Audit Trail ; hire/update/terminate Core HR audités                                                                                    | Implémenté                 | EV-AUDIT-TRAIL, EV-PROXY                                                        |
| Développement sécurisé (27001 A.8)           | SDLC sécurisé, hygiène des dépendances, maîtrise du changement           | Build TypeScript strict, migrations, CI <code>security-tests</code> (smoke/IDOR/audit:deps), Components Update + SLA, pack SDLC signé, SU Admin Security Watch + Dependabot (A.5.6) | Implémenté                 | EV-SDLC-TESTS, EV-SECURITY-WATCH, EV-ENV-SEPARATION                             |
| Durcissement réseau / applicatif             | Réduire la surface d'attaque                                             | CSP, HSTS, rate limits, garde SSRF, escape HTML, Turnstile                                                                                                                          | Implémenté                 | EV-HEADERS-CSP, EV-TURNSTILE                                                    |
| Fournisseurs / cloud (27001 A.5 ; 27017)     | Gérer la responsabilité partagée et les sous-traitants                   | Sous-traitants documentés Supabase (eu-west-1) + Vercel (dub1) ; Security Watch (CERT-FR / CISA / OSV) ; DPA client hors produit                                                    | Plateforme / sous-traitant | EV-HOSTING-REGIONS, EV-SECURITY-WATCH, EV-SUPPLIER-VERCEL, EV-SUPPLIER-SUPABASE |
| Isolation locataire (27017)                  | Séparer les données clients en multi-tenant                              | Schéma partagé + <code>organization_id</code> + RLS PostgreSQL ; périmètre API ; chemins Storage préfixés org                                                                       | Implémenté                 | EV-RLS-TENANT                                                                   |
| Administration client (27017)                | Sécuriser l'administration privilégiée et le proxy                       | Rôles Org/SU Admin ; entrée tenant SU après grant Org Admin 48 h ( <code>su_org_access_grants</code> ) ; proxy uniquement après entrée avec double attribution d'audit              | Implémenté                 | EV-PROXY, EV-SU-ORG-ACCESS, EV-RBAC-ROLES                                       |
| Protection des PII cloud (27018)             | Protéger les données à caractère personnel dans le cloud public          | Matrice de visibilité ; chiffrement ENC2 ; bucket documents privé ; régions UE ; redact PII chemins de fuite                                                                        | Implémenté                 | EV-VISIBILITY, EV-CRYPTO-FIELD, EV-DOCUMENTS                                    |
| Restitution / effacement PII (27018 / 27701) | Permettre restitution ou effacement des PII                              | Cascade de suppression d'organisation ; export DSAR + anonymisation ; purge de rétention réelle                                                                                     | Implémenté                 | EV-ORG-DELETE, EV-RETENTION                                                     |

| Thème                                | Attente                                                | Implémentation FluxeHRa                                                                                                                                            | Statut     | Preuve                                          |
|--------------------------------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------|
| Contrôles techniques privacy (27701) | Soutenir les mesures techniques d'un PIMS              | Visibilité, purge rétention, DSAR, Trust Center, field_consentss ESS + My preferences, registre Art.30. PIMS / AIPD du responsable = Client (pas un écart produit) | Implémenté | EV-PROC-NEWHIRE, EV-VISIBILITY                  |
| Adéquation fonctionnelle (25010)     | Fournir les capacités SIRH adaptées                    | Core HR bitemporel, performance, learning, compensation, analytics, intégrations — recrutement placeholder                                                         | Partiel    | EV-PROC-NEWHIRE, EV-PROC-PERF, EV-PROC-LEARNING |
| Sécurité & fiabilité (25010)         | Résister aux accès non autorisés ; comportement stable | Authz en profondeur ; rate limits ; SIEM Axiom ; backup RPO≤24h / RTO≤4h documentés. APM Sentry optionnel, non requis pour ce contrôle                             | Implémenté | EV-HEADERS-CSP, EV-HOSTING-REGIONS              |

[↑ Sommaire](#) · [↑ Languages](#)

## 9. Catalogue des processus de bout en bout

Processus SIRH clés, lien ISO, tests et preuves.

| Processus                    | Acteurs                | Routes / APIs                                                               | ISO                 | Procédure de test                                                                                    | Preuve                            |
|------------------------------|------------------------|-----------------------------------------------------------------------------|---------------------|------------------------------------------------------------------------------------------------------|-----------------------------------|
| Bootstrap locataire          | Super Admin            | /su-admin, create-organization, deploy-*, activation modules                | 27001, 27017        | Créer org démo ; vérifier schémas ; audit <code>MODULE_ACTIVATION</code>                             | EV-RBAC-ROLES, EV-AUDIT-TRAIL     |
| Auth & session               | Tous                   | /login, /{orgSlug}, session-policy, Turnstile                               | 27001, 27017        | Connexion ; idle timeout ; entêtes HSTS/CSP                                                          | EV-TURNSTILE, EV-HEADERS-CSP      |
| MFA inscription & step-up    | Admin / Super Admin    | /security/mfa, step-up login, <code>REQUIRE_MFA_FOR_PRIVILEGED_ROLES</code> | 27001, 27017        | Enrôler TOTP ; obtenir <code>aa12</code> ; sans MFA, API privilégiée → 403 <code>MFA_REQUIRED</code> | EV-AUTH-MFA                       |
| SSO OIDC org                 | Admin org + IdP        | IT Link ; /api/auth/org-oidc/*                                              | 27001, 27017        | Configurer OIDC ; se connecter via IdP                                                               | EV-SSO-OIDC                       |
| RBAC / rôles / périmètre HR  | Admin org              | Manage Roles ; <code>RequireOrgPermission</code>                            | 27001, 27017, 27701 | Attribuer permissions ; vérifier refus module                                                        | EV-RBAC-ROLES                     |
| Embauche + data request      | HR + candidat          | New hire ; /employee-data-request/{token}                                   | 27018, 27701        | Déclencher data request ; lien public ; <code>npm run test:employee-data-request</code>              | EV-PROC-NEWHIRE                   |
| MàJ employé / sortie         | HR                     | HR Self Service employé / termination                                       | 27001, 27701        | MàJ datée ; sortie ; vérifier segments historiques                                                   | EV-PROC-UPDATE, EV-PROC-TERMINATE |
| Self-service → validation HR | Employé / Manager / HR | /api/self-service/submit-change-request                                     | 27001, 27701        | Soumettre changement workflow ; notification ; application HR                                        | EV-PROC-SELFSERVICE               |

| Processus                  | Acteurs                                                           | Routes / APIs                                               | ISO                 | Procédure de test                                                                              | Preuve                      |
|----------------------------|-------------------------------------------------------------------|-------------------------------------------------------------|---------------------|------------------------------------------------------------------------------------------------|-----------------------------|
| DMS documents              | HR / Manager / Employé                                            | <code>/api/documents/*</code> , bucket privé                | 27001, 27018, 27701 | Upload ; téléchargement non autorisé refusé ; stream via route fichier                         | EV-DOCUMENTS                |
| Visibilité & rétention     | Admin org / SU                                                    | UI Data Visibility & Retention                              | 27018, 27701, 25010 | Régler visibilité et <code>retentionMonths</code> ; lancer analyse/purge rétention             | EV-VISIBILITY, EV-RETENTION |
| Mass upload / rollback     | HR / Admin                                                        | APIs mass upload ; audit                                    | 27001, 25010        | Commit CSV ; rollback ; vérifier audit                                                         | EV-PROC-MASSUPLOAD          |
| Cycle campagne performance | HR / Manager / Employé                                            | Campagnes, documents, signature, push Core HR               | 25010, 27001        | <code>npm run test:performance-smoke</code> ou tests <code>lib/performance/__tests__</code>    | EV-PROC-PERF                |
| Learning & attestations    | Admin / Apprenant / Manager                                       | Learning admin, player, cron compliance                     | 25010, 27001        | Inscrire ; terminer SCORM/attestation ; dashboard conformité                                   | EV-PROC-LEARNING            |
| Export intégrations        | Admin org / M2M                                                   | <code>/api/integrations/export</code> , SFTP, HMAC          | 27001, 27017, 27018 | Régénérer clé ; export Bearer + HMAC signé avec cette clé ; empreinte d'audit seulement        | EV-INTEGRATIONS             |
| Proxy / impersonation      | SU avec grant org 48 h actif, ou Org Admin / HR dans le périmètre | <code>/api/proxy/*</code> , <code>/api/su-org-access</code> | 27001, 27017        | Demander/approuver accès SU ; Enter org ; démarrer proxy ; JWT = utilisateur réel ; audit dual | EV-PROXY, EV-SU-ORG-ACCESS  |
| Suppression organisation   | Super Admin                                                       | <code>/api/admin/delete-organization</code>                 | 27701, 27018        | Sur org jetable uniquement : supprimer ; vérifier purge                                        | EV-ORG-DELETE               |
| Revue audit trail          | Admin org / SU                                                    | Onglet Audit Trail                                          | 27001, 27701        | Filtrer ; exporter CSV ; vérifier lignes proxy                                                 | EV-AUDIT-TRAIL              |

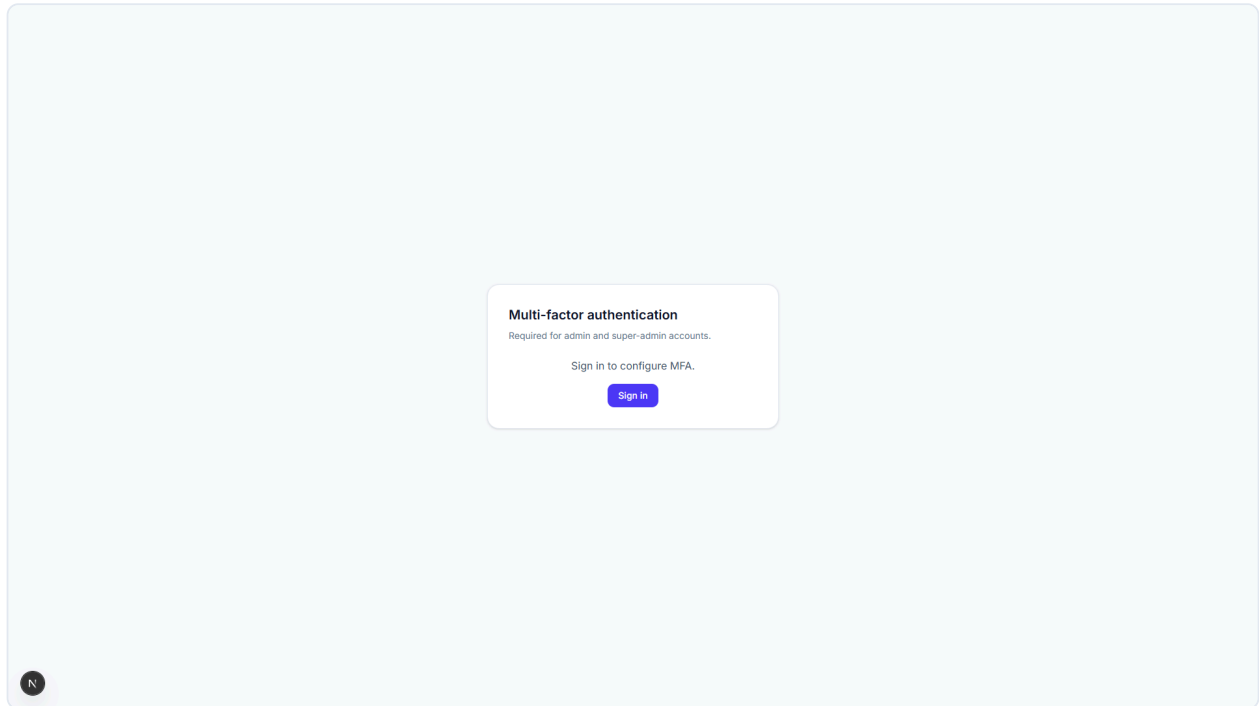
[↑ Sommaire](#) · [↑ Languages](#)

## 10. Pack de preuves — comment démontrer

Pour chaque ID : quoi montrer, comment tester, références code, et emplacement figure (remplacer les SVG par des captures réelles — voir `docs/iso-evidence-capture-checklist.md`).

## EV-AUTH-MFA — MFA TOTP & step-up privilégié

- **Montrer:** Page `/security/mfa`; login MFA challenge; Vercel env `REQUIRE_MFA_FOR_PRIVILEGED_ROLES`
- **Tester:** Enroll authenticator; complete step-up to JWT `aa12`; call privileged API without MFA → 403 `MFA_REQUIRED`
- **Code / config:** `lib/auth-mfa-policy.ts`, `lib/mfa-step-up.ts`, `app/security/mfa/page.tsx`



EV-AUTH-MFA — MFA TOTP & step-up privilégié (screenshot)

## EV-PASSWORD-POLICY — Règles & messages de mot de passe

- **Montrer:** Login → Forgot password notice; /reset-password form; welcome/reset emails
- **Tester:** Reject short/weak password on set/reset; existing passwords continue to work until changed
- **Code / config:** lib/password-policy.ts, app/reset-password/page.tsx, components/sign-in-panel.tsx, lib/templated-auth-email.ts

FluxeHRa

fr

**FluxeHRa**

Sign in to access your workspace.

**Reset password** [Back to sign in](#)

We will email you a link to set a new password. The same message is shown whether or not the email is registered, to protect your account information.

When you set a new password: At least 12 characters, with uppercase, lowercase, a digit, and a special character. Existing passwords continue to work until you change them.

Email address

you@company.com

Success!

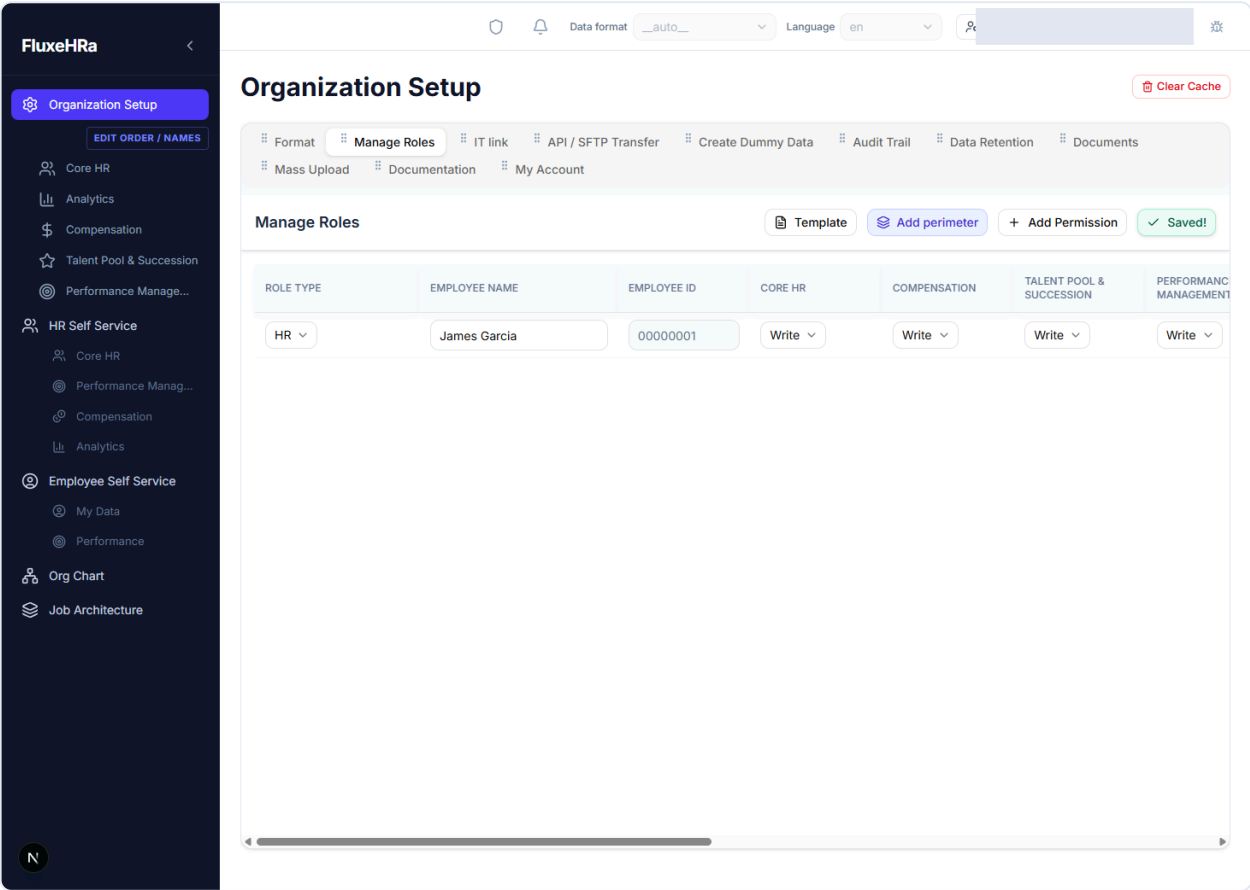
[Send reset link](#)

[Privacy Policy](#) [Terms of Use](#) [Trust Center](#)

EV-PASSWORD-POLICY — Règles & messages de mot de passe (screenshot)

EV-RBAC-ROLES — Matrice rôles & permissions

- **Montrer:** Org-setup → Manage Roles; SU Admin org/admins
- **Tester:** Remove module write; confirm UI gate and API 403
- **Code / config:** lib/org-permissions.ts, components/manage-roles-tab.tsx, lib/supabase-api-auth.ts



EV-RBAC-ROLES — Matrice rôles & permissions (screenshot)

## EV-RLS-TENANT — Isolation multi-tenant RLS

- **Montrer:** Attempt cross-org data access (second org user)
- **Tester:** Query/API against foreign `organization_id` returns empty/denied; review RLS migrations
- **Code / config:** `supabase/migrations/20260606120000_*, 20260610120000_*, scripts/sql/rls-inventory.sql`

EV-RLS-TENANT

### Multi-tenant RLS isolation

```
Tenant boundary: organization_id enforced in Postgres RLS policies.
Inventory helper: scripts/sql/rls-inventory.sql

-- Read-only RLS inventory (plan "Remédiation sécurité juin 2026", item 9).
-- Run in Supabase Dashboard > SQL Editor (or psql) on project zlsruhdxyfwqfpzckg.
-- No writes are performed.

-- 1. RLS enabled / forced per table (public schema)
select
  n.nspname as schema,
  c.relname as table name,
  c.relrowsecurity as rls_enabled,
  c.relforcerowsecurity as rls_forced
from pg_class c
join pg_namespace n on n.oid = c.relnamespace
where n.nspname = 'public'
and c.relkind = 'r'
order by c.relname;

-- 2. All policies on public tables
select
  schemaname,
  tablename,
  policyname,
  permissive,
  roles,
  cmd,
  qual,
  with_check
from pg_policies
where schemaname = 'public'
order by tablename, policyname;

-- 3. Focus: legacy tables flagged by the June 2026 audit
select
  tablename,
  policyname,
  permissive,
```

Generated evidence card — FluxeHRA ISO Alignment Pack

## EV-RLS-TENANT — Isolation multi-tenant RLS (screenshot)

## EV-CRYPTO-FIELD — Chiffrement des champs sensibles

- **Montrer:** Save SSN/IBAN; inspect DB value prefix `ENC2::`
- **Tester:** Encrypt/decrypt via authorized role; non-privileged decrypt limited to own/team ciphertext
- **Code / config:** `lib/encryption-core.ts`, `app/api/crypto/*`, `lib/crypto-route-auth.ts`

EV-CRYPTO-FIELD

### Sensitive field encryption (ENC2::)

```
Application ciphertext prefix: ENC2:: (AES-GCM)
Source: lib/encryption-core.ts
Decrypt gated by role / ownership (lib/crypto-route-auth.ts)

Demo note: never capture plaintext SSN/IBAN in customer packs.
DB inspection should show only ENC2::... values for sensitive columns.
```

Generated evidence card — FluxeHra ISO Alignment Pack

EV-CRYPTO-FIELD — Chiffrement des champs sensibles (screenshot)

EV-AUDIT-TRAIL — UI journal d’audit

- **Montrer:** Org-setup / SU → Audit Trail
- **Tester:** Perform audited action (mass upload, settings); confirm event row; CSV export
- **Code / config:** lib/audit-server.ts, lib/audit-client.ts, components/audit-trail-tab.tsx

FluxeHRa

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Organization Setup

Format

Manage Roles

IT link

API / SFTP Transfer

Create Dummy Data

Audit Trail

Data Retention

Documents

Mass Upload

Documentation

My Account

Audit Trail

mm/dd/yyyy

to

mm/dd/yyyy

Search logs...

Compliance evidence

Export CSV

| DATE & TIME           | PAGE / MODULE                               | ACTION (REASON) | DETAILS                                         |
|-----------------------|---------------------------------------------|-----------------|-------------------------------------------------|
| Aug 10, 2026 17:18:29 | /fluxehra/org-se<br>tup                     | PAGE_VIEW       | Visited /fluxehra/org-setup                     |
| Aug 10, 2026 17:14:15 | /fluxehra/hr-self<br>-service/core-hr       | PAGE_VIEW       | Visited /fluxehra/hr-self-<br>service/core-hr   |
| Aug 10, 2026 17:14:03 | /fluxehra/org-se<br>tup                     | PAGE_VIEW       | Visited /fluxehra/org-setup                     |
| Aug 10, 2026 17:13:50 | /fluxehra/hr-self<br>-service/docum<br>ents | PAGE_VIEW       | Visited /fluxehra/hr-self-<br>service/documents |
| Aug 7, 2026 22:32:50  | /fluxehra/hr-self<br>-service/docum<br>ents | PAGE_VIEW       | Visited /fluxehra/hr-self-<br>service/documents |
| Aug 7, 2026 22:32:43  | /fluxehra/hr-self<br>-service/core-hr       | PAGE_VIEW       | Visited /fluxehra/hr-self-<br>service/core-hr   |
| Aug 7, 2026 22:32:28  | /fluxehra/org-ch<br>art                     | PAGE_VIEW       | Visited /fluxehra/org-chart                     |
| Aug 7, 2026 22:17:18  | /fluxehra/org-ch<br>art                     | PAGE_VIEW       | Visited /fluxehra/org-chart                     |
| Aug 7, 2026 22:15:16  | /fluxehra/org-ch<br>art                     | PAGE_VIEW       | Visited /fluxehra/org-chart                     |

Showing 1-20 of 339

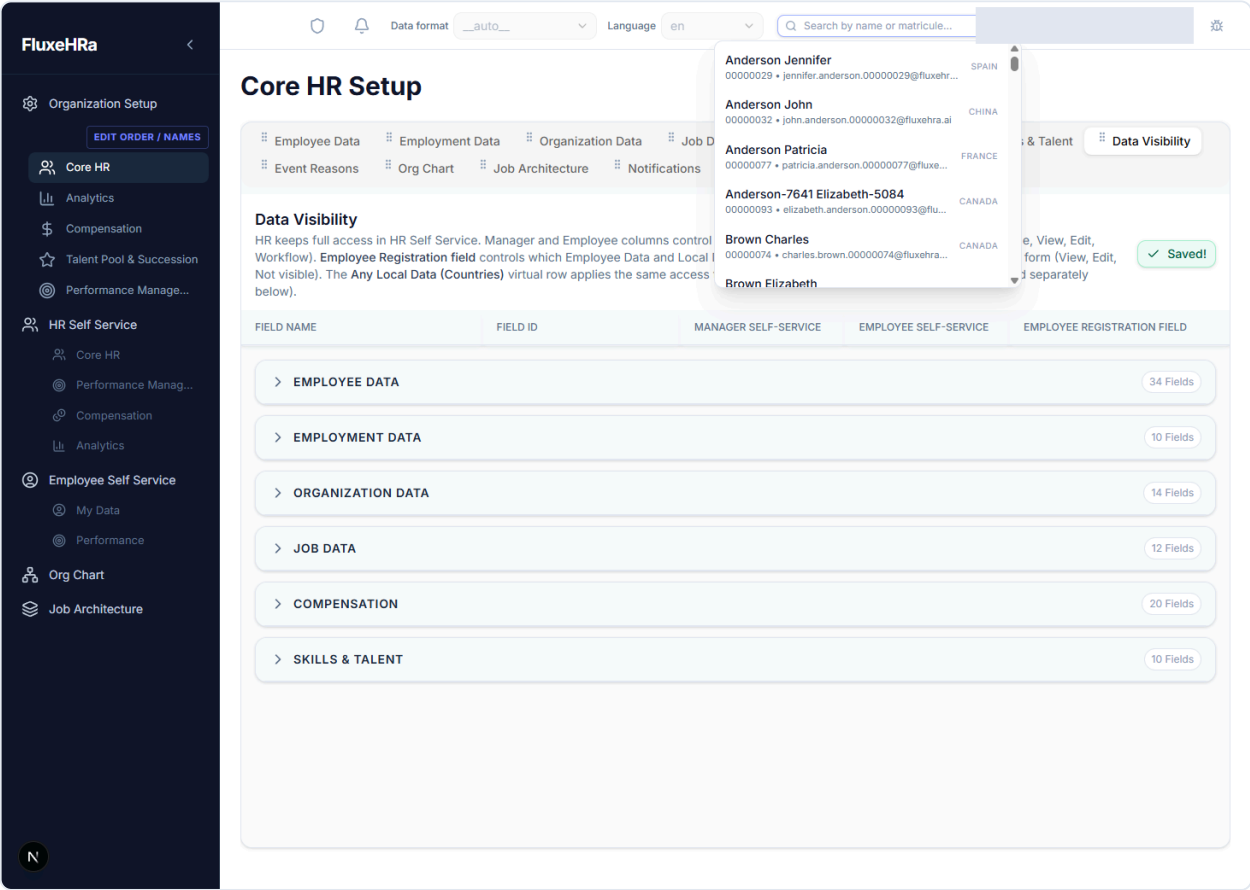
Per page 20

< 1 2 3 ... 17 >

EV-AUDIT-TRAIL — UI journal d’audit (screenshot)

EV-PROXY — Responsabilité du proxy

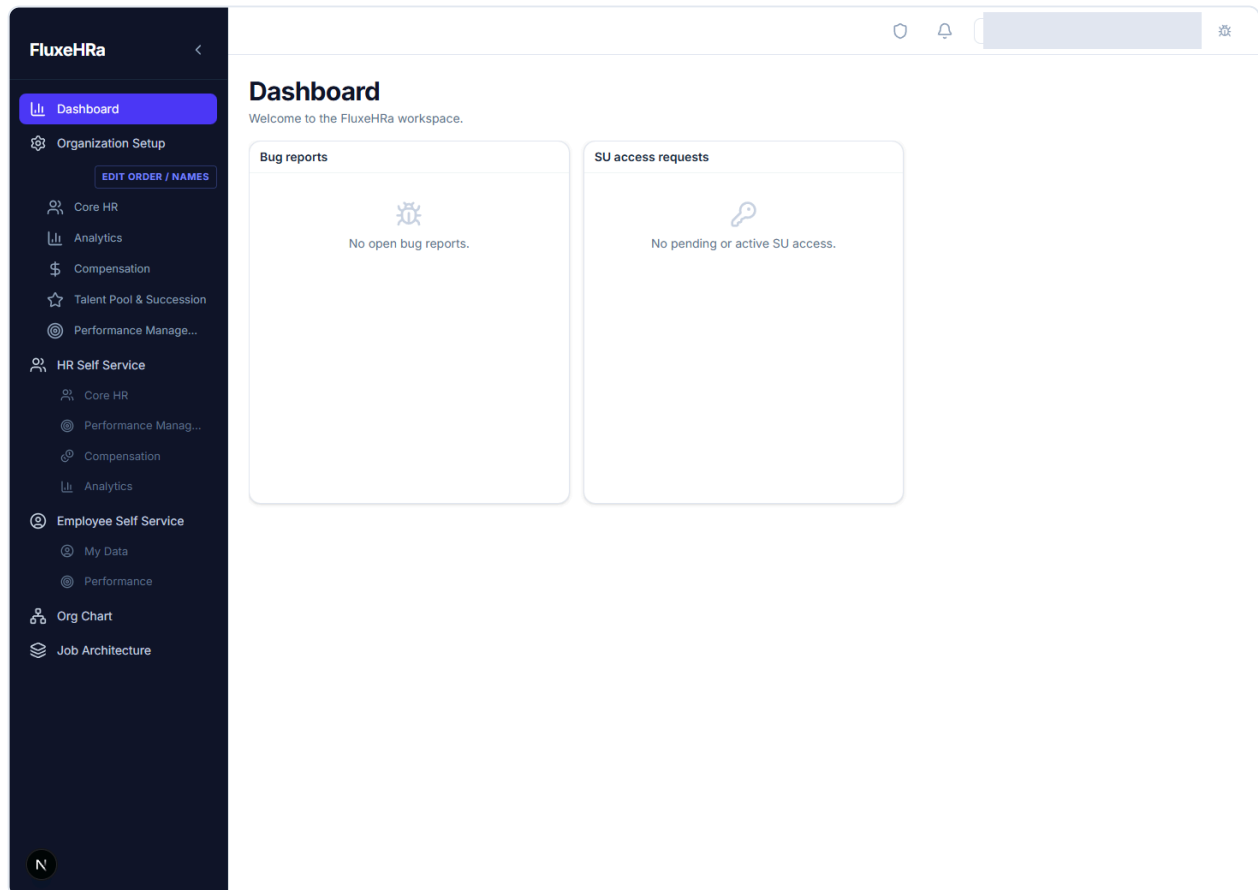
- **Montrer:** Proxy session banner; audit with proxied identity
- **Tester:** With active SU grant (or org privileged role): start/end proxy; confirm continuous eligibility re-check; dual identity in logs
- **Code / config:** `lib/proxy-server.ts`, `lib/proxy-api-guard.ts`, `lib/su-org-access.ts`



EV-PROXY — Responsabilité du proxy (screenshot)

## EV-SU-ORG-ACCESS — Grants d'accès SU aux orgs (48 h)

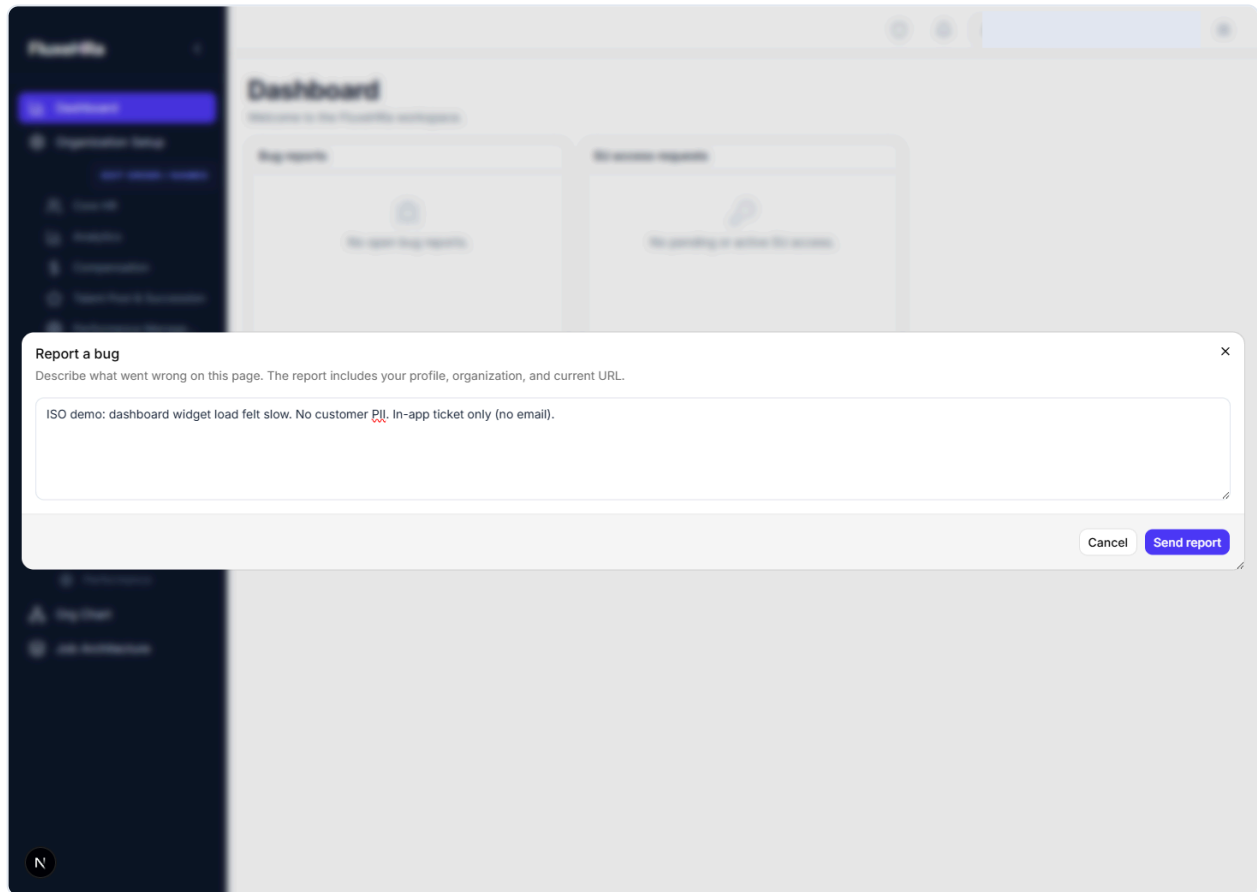
- **Montrer:** SU Enter Organisation → Request; Org Admin Dashboard → Accept/Deny; emerald authorized orgs
- **Tester:** Approve grant; Enter org; confirm middleware/API deny without grant for data paths; expire after 48h kicks SU out. Deploy-schema to orgs does NOT require grant (config only, no PII read).
- **Code / config:** `su_org_access_grants` , `/api/su-org-access` , `has_active_su_org_grant`



EV-SU-ORG-ACCESS — Grants d'accès SU aux orgs (48 h) (screenshot)

## EV-BUG-ESCALATION — Escalade des bugs manuels

- **Montrer:** Report a bug → HR / Org Admin / SU Dashboard widgets
- **Tester:** Submit manual bug (ticket, no email); Forward HR→Admin→SU; Clear; auto client errors still email SMTP
- **Code / config:** `bug_report_tickets`, `/api/bug-report`, `/api/bug-reports`



EV-BUG-ESCALATION — Escalade des bugs manuels (screenshot)

EV-VISIBILITY — Matrice de visibilité des données

- **Montrer:** Core HR / Data Visibility; ESS field hidden vs HR visible
- **Tester:** Set field to `none` for employee; confirm self-service omit/deny
- **Code / config:** `lib/field-visibility.ts`, `lib/self-service-submit-auth.ts`

FluxeHRA

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Core HR Setup

Employee Data Employment Data Organization Data Job Data Compensation Local Data Skills & Talent Data Visibility

Event Reasons Org Chart Job Architecture Notifications

Data Visibility

HR keeps full access in HR Self Service. Manager and Employee columns control Manager Self Service and Employee Self Service (None, View, Edit, Workflow). Employee Registration field controls which Employee Data and Local Data fields appear on the hired-employee data request form (View, Edit, Not visible). The Any Local Data (Countries) virtual row applies the same access to every country-specific Local Data schema (not listed separately below).

Field NameField IDManager Self-ServiceEmployee Self-ServiceEmployee Registration Field

Employee Data34 Fields

Employment Data10 Fields

Organization Data14 Fields

Job Data12 Fields

Compensation20 Fields

Skills & Talent10 Fields

EV-VISIBILITY — Matrice de visibilité des données (screenshot)

EV-RETENTION — Configuration de rétention & purge

- **Montrer:** Retention months per field; document type retention; analyze/purge actions
- **Tester:** Configure retention; run Retention analysis; purge expired values; confirm RETENTION\_\* audit events
- **Code / config:** `lib/retention-purge.ts`, `/api/hr/retention`, field-visibility retention tab

FluxeHRa

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Organization Setup

Clear Cache

Format Manage Roles IT link API / SFTP Transfer Create Dummy Data Audit Trail Data Retention Documents

Mass Upload Documentation My Account

Data Retention

Retention analysis

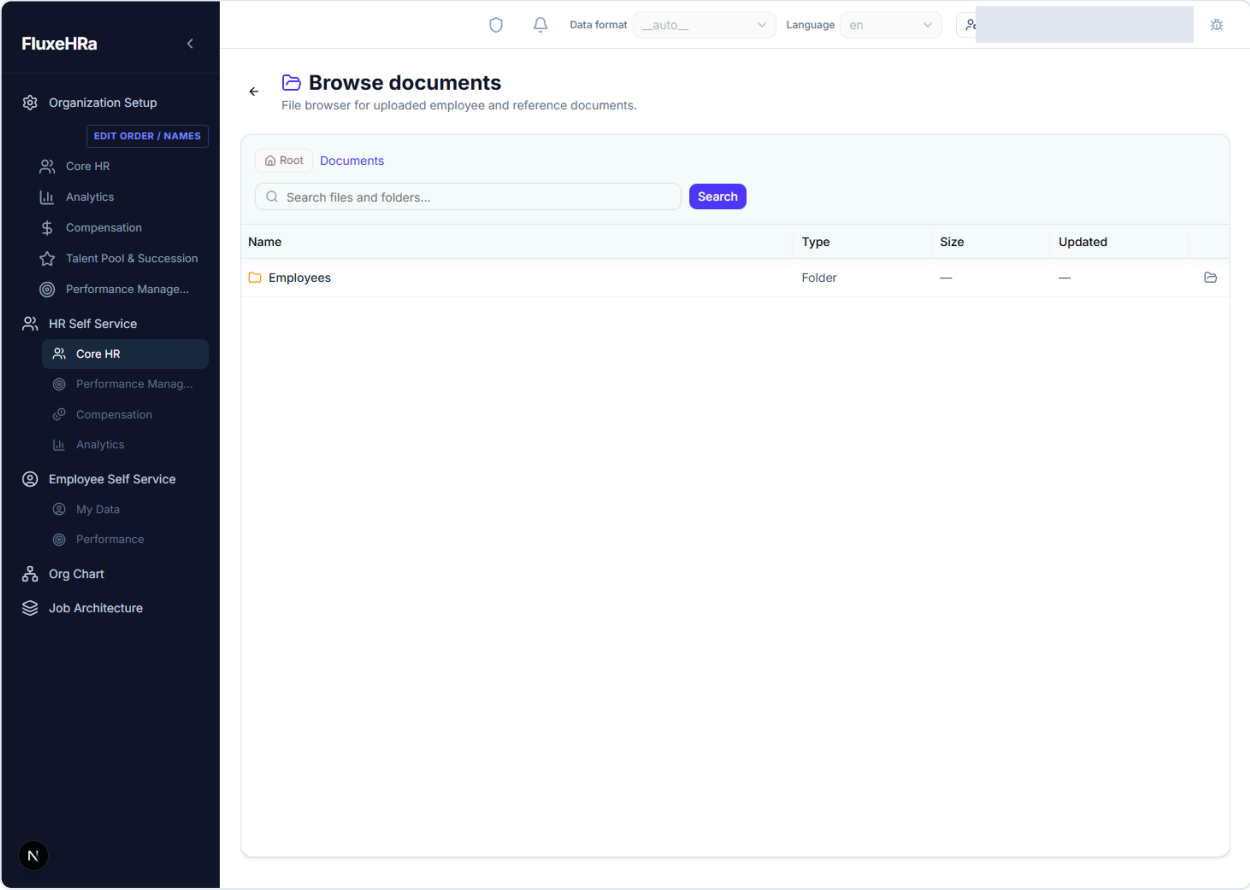
✓ Saved!

| FIELD NAME          | FIELD ID | RETENTION LENGTH (MONTHS AFTER DEPARTURE) | NUMBER OF ITEMS |
|---------------------|----------|-------------------------------------------|-----------------|
| CORE HR             |          |                                           |                 |
| > EMPLOYEE DATA     |          |                                           | 34 Fields       |
| > EMPLOYMENT DATA   |          |                                           | 10 Fields       |
| > ORGANIZATION DATA |          |                                           | 14 Fields       |
| > JOB DATA          |          |                                           | 12 Fields       |
| > COMPENSATION      |          |                                           | 20 Fields       |
| > SKILLS & TALENT   |          |                                           | 10 Fields       |
| ANALYTICS           |          |                                           |                 |
| > ANALYTICS         |          |                                           | 0 Fields        |
| COMPENSATION        |          |                                           |                 |

EV-RETENTION — Configuration de rétention & purge (screenshot)

EV-DOCUMENTS — Accès documents privés

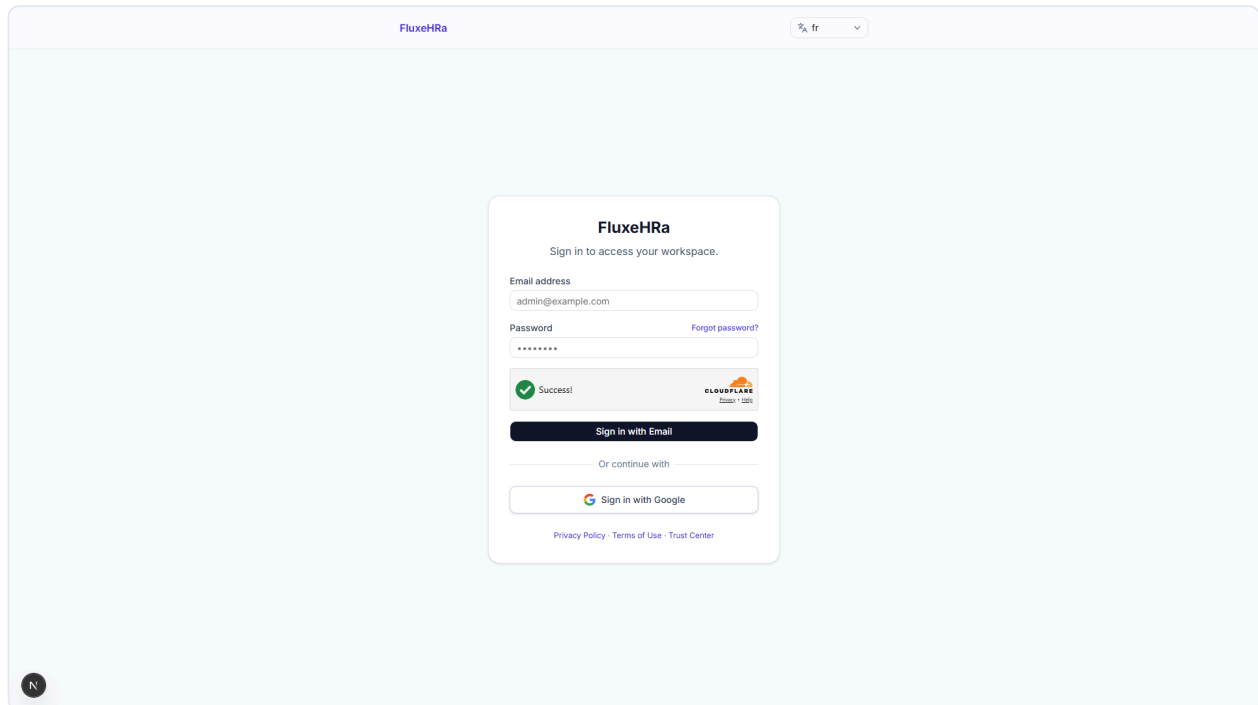
- **Montrer:** Upload under employee; download via app only
- **Tester:** Direct storage URL without auth fails; authorized `/api/documents/file/...` succeeds; scoped HR denied outside regional perimeter on direct URL
- **Code / config:** `lib/document-access.ts`, `lib/storage-ops.ts`, migration documents bucket private



EV-DOCUMENTS — Accès documents privés (screenshot)

## EV-TURNSTILE — Protection anti-bot (Turnstile)

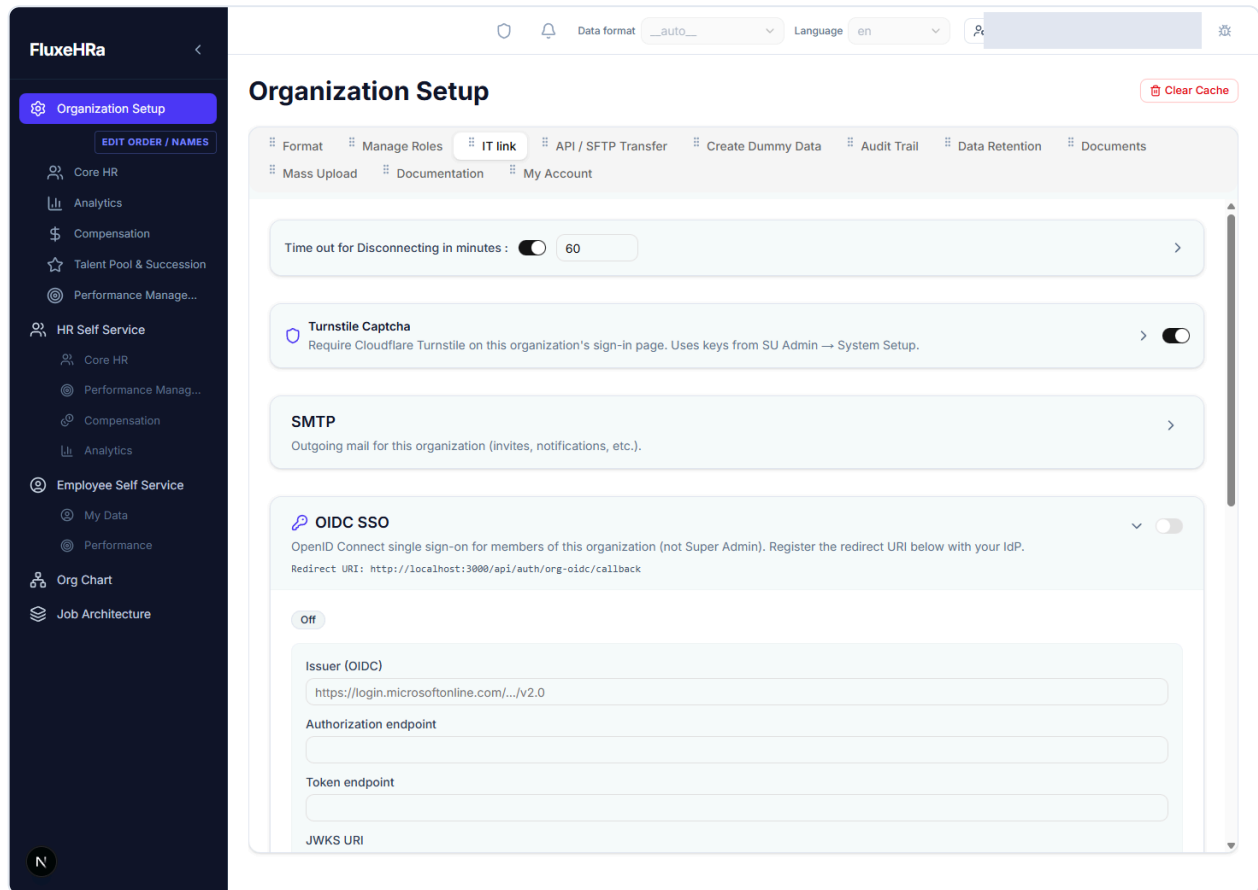
- **Montrer:** SU System Setup / Org IT Link Turnstile toggle; login challenge
- **Tester:** Enable Turnstile; blocked without token on check-email / forgot-password
- **Code / config:** `lib/turnstile-server.ts`, `lib/turnstile-settings.ts`



EV-TURNSTILE — Protection anti-bot (Turnstile) (screenshot)

## EV-SSO-OIDC — SSO OIDC par organisation

- **Montrer:** Org-setup → IT Link SSO settings
- **Tester:** Authorize + callback with HMAC state; invalid redirect rejected
- **Code / config:** `app/api/auth/org-oidc/*`, `lib/org-oidc-state.ts`, `lib/app-origin.ts`



EV-SSO-OIDC — SSO OIDC par organisation (screenshot)

## EV-ESIGN-FLUXEHRA — E-signature FluxeHRa (eIDAS SES + PAdES-B optionnel)

- **Montrer:** SU Setup platform toggle; Org IT Link (expiry, OTP, consent, company signatories); public `/sign/[token]`; HR evidence Certificate/JSON; optional PAdES seal
- **Tester:** Send envelope; open link; OTP if required; consent; draw/type; complete stamped PDF; download SES evidence pack; exclusivity disables DocuSign; optional PAdES-B `ETSI.CAdES.detached`
- **Code / config:** `lib/esign/*`, `lib/esign-provider.ts`, `docs/esign-standards.md`, `app/api/public/esign/*`, migrations through `20260929210000_esign_audit_pades.sql`

### Evidence placeholder

EV-ESIGN-FLUXEHRA

Replace with screenshot — see `docs/iso-evidence-capture-checklist.md`

FluxeHRa ISO Alignment Pack

EV-ESIGN-FLUXEHRA — E-signature FluxeHRa (eIDAS SES + PAdES-B optionnel) (placeholder)

## EV-DOCUSIGN — Signature DocuSign (optionnelle)

- **Montrer:** SU Setup DocuSign + Org IT Link Account/User ID + Grant consent
- **Tester:** Sandbox send + Connect completed webhook; exclusivity disables Fluxehra e-signature
- **Code / config:** `lib/docusign-*.ts`, `app/api/hr/docusign/*`, `/api/integrations/docusign/webhook`

### Evidence placeholder

EV-DOCUSIGN

Replace with screenshot — see docs/iso-evidence-capture-checklist.md

FluxeHRa ISO Alignment Pack

EV-DOCUSIGN — Signature DocuSign (optionnelle) (placeholder)

## EV-INTEGRATIONS — Sécurité des exports d'intégration

- **Montrer:** Org-setup → API / SFTP; regenerate key once
- **Tester:** Export with Bearer integration key + HMAC headers (per-key secret); rate limit; audit stores fingerprint not payload
- **Code / config:** `lib/integration-api-key.ts`, `lib/integration-export-*.ts`

The screenshot shows the 'Organization Setup' page in the FluxeHRA application. The left sidebar contains a navigation menu with options like 'Core HR', 'Analytics', 'Compensation', 'Talent Pool & Succession', 'Performance Manage...', 'HR Self Service', 'Employee Self Service', 'Org Chart', and 'Job Architecture'. The main content area is titled 'Organization Setup' and has a 'Clear Cache' button. Below the title is a horizontal menu with tabs: 'Format', 'Manage Roles', 'IT link', 'API / SFTP Transfer' (selected), 'Create Dummy Data', 'Audit Trail', 'Data Retention', and 'Documents'. The 'API / SFTP Transfer' tab is active, showing a 'New API / SFTP' section with a '+ New API Key' button. The main configuration area is titled 'API Credentials & Webhook' and includes fields for 'Integration Name' (set to 'New API Key'), 'API key' (displayed as 'fx\_M6EK...Z0VD' with a 'Renew key' button), 'Export IP allowlist (optional)' (set to '203.0.113.10, 198.51.100.0'), 'Push Destination (Webhook)' (set to 'https://api.external-system.com/webhook/hr'), and 'Data Transfer Type' (with options for 'Full Transfer' and 'Incremental Transfer').

EV- INTEGRATIONS — Sécurité des exports d'intégration (screenshot)

## EV-HEADERS-CSP — En-têtes de sécurité & CSP

- **Montrer:** Browser DevTools → Response headers on any authenticated page
- **Tester:** Confirm CSP nonce, HSTS, X-Frame-Options DENY, nosniff
- **Code / config:** `lib/csp.ts`, `proxy.ts`, `next.config.js`

EV-HEADERS-CSP

### Security response headers

```
GET http://127.0.0.1:3000/trust
status: 200

content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'
https://challenges.cloudflare.com https://va.vercel-scripts.com; style-src 'self' 'unsafe-
inline'; img-src 'self' data: blob: https://*.supabase.co; font-src 'self' data; connect-src
'self' https://*.supabase.co wss://*.supabase.co https://challenges.cloudflare.com
https://vitals.vercel-insights.com; frame-src 'self' https://challenges.cloudflare.com; object-
src 'none'; base-uri 'self'; form-action 'self'; frame-ancestors 'none'
strict-transport-security: max-age=63072000; includeSubDomains; preload
x-frame-options: DENY
x-content-type-options: nosniff
referrer-policy: strict-origin-when-cross-origin
permissions-policy: camera=(), microphone=(), geolocation=(), payment=()
x-dns-prefetch-control: on
```

Generated evidence card — FluxeHra ISO Alignment Pack

EV-HEADERS-CSP — En-têtes de sécurité & CSP (screenshot)

EV-HOSTING-REGIONS — Alignement d'hébergement UE

- **Montrer:** Supabase project region; vercel.json region dub1
- **Tester:** Document eu-west-1 + dub1 in customer processing register
- **Code / config:** vercel.json , .env.example , security whitepaper § hosting

FluxeHRa

Centre de confiance

fr

### Centre de confiance

Contrôles de sécurité techniques, régions d'hébergement et documents d'assurance téléchargeables pour les équipes IT, RSSI et DPO. FluxeHRa couvre Core RH, Performance, Formation, Analytique et Rémunération sur une stack multi-tenant UE (Supabase Irlande, Vercel Dublin). FluxeHRa n'est pas certifié ISO du seul fait de ces documents — voir le pack d'alignement ISO pour un statut honnête des contrôles.

#### Downloads

Télécharger le livre blanc sécurité IT (PDF)

Télécharger le pack d'alignement ISO (PDF)

White paper (HTML) - ISO pack (HTML)

Télécharger le pack support AIPD / DPIA

Télécharger le DPA

Télécharger les conditions générales

Télécharger les conditions d'utilisation

#### Hosting & sub-processors

- **Supabase** — PostgreSQL, Auth, Storage (production region eu-west-1 , Ireland)
- **Vercel** — Next.js application & API ( dub1 , Dublin)

Full list: [sub-processors note](#).

#### Privacy & DPA

Read our [Politique de confidentialité](#) for website visitors and application users. Customers typically act as controller for employee personal data; FluxeHRa acts as processor. For a Data Processing Agreement (DPA) or privacy questions, contact [contact@fluxehra.ai](mailto:contact@fluxehra.ai). The current DPA and legal documents are available as downloadable files above.

EV-HOSTING-REGIONS — Alignement d'hébergement UE (screenshot)

## EV-PROC-NEWHIRE — Embauche & data request

- **Montrer:** HR Self Service → New Hire; public token page
- **Tester:** `npm run test:employee-data-request`; manual 90-day token expiry
- **Code / config:** `lib/employee-data-request-*.ts`, public EDR APIs

**FluxeHRA**

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

**New Hire (Manual)**

Create a new employee record across all schemas.

Save as draft Request Hired Employee Data Complete Hire

Contract for signature Select employee country first Preview Send for Signature

**Event Details**

Effective Date (Hire Date) \* 08/10/2026 Event Reason \* NEW\_HIRE Country \* Select Country

> EMPLOYEE DATA 34 Fields

> EMPLOYMENT DATA 10 Fields

> ORGANIZATION 14 Fields

> JOB DATA 12 Fields

> COMPENSATION 20 Fields

EV-PROC-NEWHIRE — Embauche & data request (screenshot)

EV-PROC-UPDATE — Mise à jour bitemporelle employé

- **Montrer:** HR employee record with effective dating
- **Tester:** Split history on mid-period change; verify prior segment retained
- **Code / config:** lib/temporal-data.ts

FluxeHRa

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

N

Data format

\_\_auto\_\_

Language

en

←

ID: 00000014 • Status: Active

Export DSAR

Anonymize

<

>

History

Current (2026-08-10)

Save Changes

> EMPLOYEE DATA

34 Fields

> EMPLOYMENT DATA

10 Fields

> ORGANIZATION

14 Fields

> JOB DATA

12 Fields

> COMPENSATION

20 Fields

> LOCAL DATA

6 Fields

> SKILLS & TALENT

10 Fields

EV-PROC-UPDATE — Mise à jour bitemporelle employé (screenshot)

## EV-PROC-TERMINATE — Sortie / termination

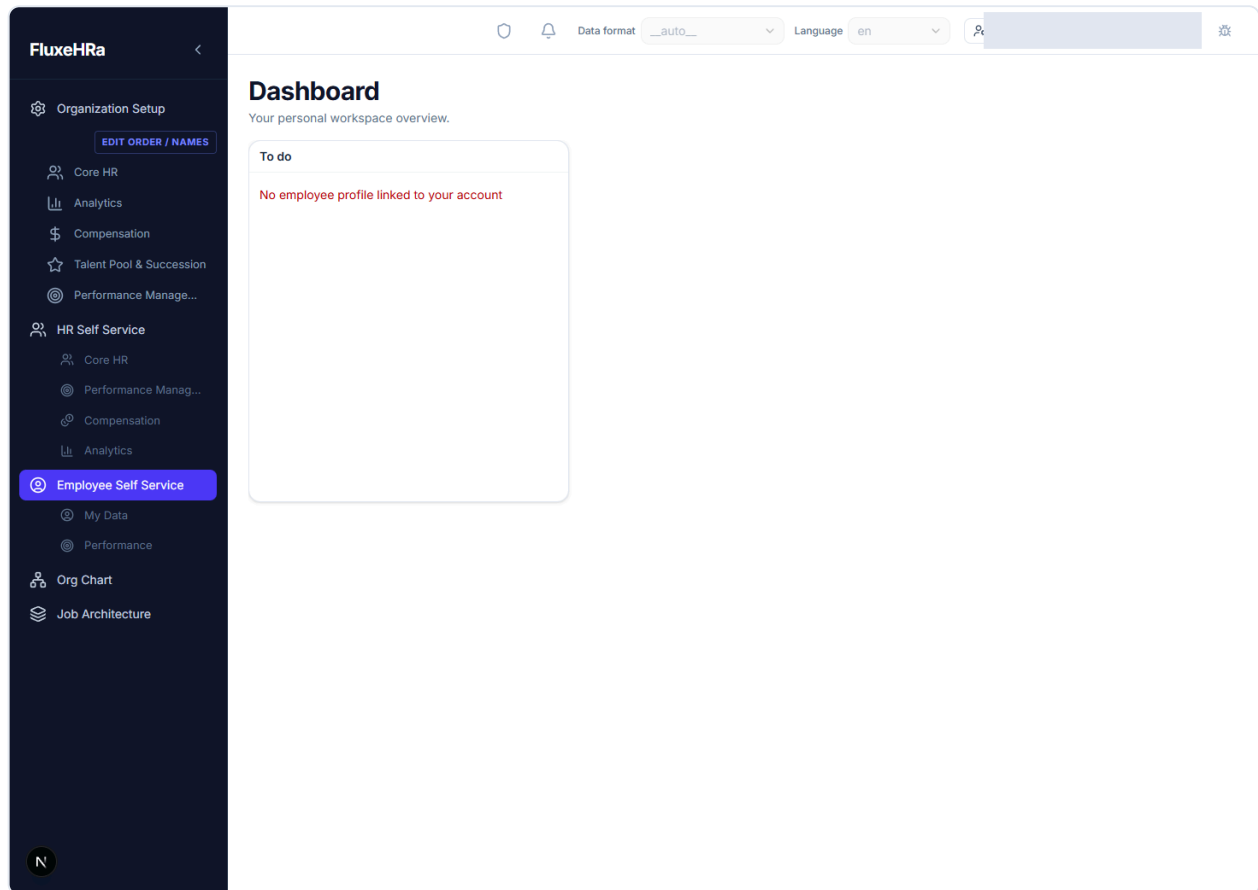
- **Montrer:** HR Self Service → Termination
- **Tester:** Set end dates/status; confirm lifecycle event
- **Code / config:** HR termination route under `hr-self-service/termination`

The screenshot displays the 'Employee Termination' process in the FluxeHRa system. The interface is divided into a left sidebar and a main content area. The sidebar, titled 'FluxeHRa', contains a navigation menu with categories like 'Organization Setup', 'HR Self Service', 'Employee Self Service', 'Org Chart', and 'Job Architecture'. The 'HR Self Service' category is expanded, showing 'Core HR' as the selected option. The main content area is titled 'Employee Termination' with the subtitle 'Process an employee departure.' and a 'Process Termination' button. It features a 'Select Employee' section with a search bar labeled 'Search Active Employees...'. Below this is the 'Termination Details' section, which includes an 'Effective Date' field set to '08/10/2026' and a 'Termination Reason' dropdown menu set to 'RESIGNATION'. The 'Termination Reason' dropdown also shows 'Category: Termination'.

EV-PROC-TERMINATE — Sortie / termination (screenshot)

## EV-PROC-SELFSERVICE — Demande de changement self-service

- **Montrer:** My Data / My Team workflow fields; HR notification
- **Tester:** Submit change; approve/apply as HR
- **Code / config:** `lib/self-service-submit-auth.ts`



EV-PROC-SELFSERVICE — Demande de changement self-service (screenshot)

## EV-PROC-MASSUPLOAD — Mass upload & rollback

- **Montrer:** Mass Upload tab; batch list
- **Tester:** Commit then delete/rollback batch; audit events present
- **Code / config:** `/api/admin/mass-upload/*`

FluxeHRA

Organization Setup

EDIT ORDER / NAMES

Core HR

Analytics

Compensation

Talent Pool & Succession

Performance Manage...

HR Self Service

Core HR

Performance Manag...

Compensation

Analytics

Employee Self Service

My Data

Performance

Org Chart

Job Architecture

Organization Setup

Clear Cache

Format

Manage Roles

IT link

API / SFTP Transfer

Create Dummy Data

Audit Trail

Data Retention

Documents

Mass Upload

Documentation

My Account

Mass Upload for a Domain

Upload a full module slice (all uploadable fields) for existing employees. For Core HR, one file covers all schema tabs except Local Data (use the per-tab flow if you need local country-specific fields). CSV headers use field IDs; include `employee_id` with the in-app Employee ID (not the Supabase UUID).

Upload name

Domain (module)

Effective date

Event category

Sub-reason

Q1 job data refresh

Core HR

08/10/2026

Hire / Rehire

NEW\_HIRE

Same-day order

First

Last

Download sample

Browse CSV

Upload & save

Mass Upload for specific field(s)

Pick one or more fields; the sample CSV always includes `employee_id` for matching.

Upload name

Domain (module)

Schema tab

Effective date

Event category

Salary correction batch

Core HR

employee-data

08/10/2026

Hire / Rehire

Sub-reason

NEW\_HIRE

Fields

Select field

Add field

Same-day order

First

Last

Download sample

Browse CSV

Upload & save

Delete a Mass Upload for a Domain

EV-PROC-MASSUPLOAD — Mass upload &amp; rollback (screenshot)

## EV-PROC-PERF — Campagne performance

- **Montrer:** Performance Management campaign → document → sign
- **Tester:** `npm test` (performance unit tests); optional `npm run test:performance-smoke`
- **Code / config:** `lib/performance/` , `app/api/performance/`

The screenshot shows the FluxeHRA web application interface. On the left is a dark sidebar with navigation links: Organization Setup, Core HR, Analytics, Compensation, Talent Pool & Succession, Performance Management (selected), HR Self Service, Employee Self Service, My Data, Performance, Org Chart, and Job Architecture. The main content area is titled 'Performance Management' and includes a toggle for 'Performance Management activation'. Below this are tabs for 'Performance Reviews', 'Goals & Objectives', and 'Continuous Feedback'. The 'Performance Reviews' tab is active, showing a 'SAVED TEMPLATES' section for '2027 — Default Performance'. It has radio buttons for 'Closed (pushed)', 'In setup', and 'Mass created'. Below is a form with 'Campaign Name' (Default Performance) and 'Campaign Year' (2027), with a 'Saved!' confirmation. A breadcrumb trail shows 'Define Fields > Define Templates > Define Process > Manage Process'. At the bottom, there's a toggle for 'Link two campaigns of the same year' and a note: 'A second campaign of the same year is required to link.' Action buttons include 'Mass Create', 'Move all to', 'Opened', 'Download all data from selected campaign', and 'Push to Core HR'.

EV-PROC-PERF — Campagne performance (screenshot)

## EV-PROC-LEARNING — Conformité Learning

- **Montrer:** Learning admin + team compliance tab
- **Tester:** Enroll; progress; attestation; compliance dashboard
- **Code / config:** `app/api/learning/` , `/api/cron/learning-compliance`

### Evidence placeholder

EV-PROC-LEARNING

Replace with screenshot — see docs/iso-evidence-capture-checklist.md

FluxeHRa ISO Alignment Pack

EV-PROC-LEARNING — Conformité Learning (placeholder)

## EV-ORG-DELETE — Cascade de suppression d'organisation

- **Montrer:** SU Admin delete organization (disposable org only)
- **Tester:** Confirm cascade removes org tables, storage prefixes, member auth users
- **Code / config:** `lib/delete-organization-cascade.ts`

### Evidence placeholder

EV-ORG-DELETE

Replace with screenshot — see docs/iso-evidence-capture-checklist.md

FluxeHRa ISO Alignment Pack

EV-ORG-DELETE — Cascade de suppression d'organisation (placeholder)

## EV-SDLC-TESTS — Tests automatisés & preuves de changement

- **Montrer:** CI/local test run output; migration history
- **Tester:** `npm test`; `npm run test:employee-data-request`; `npm run lint`; GitHub `security-tests` workflow
- **Code / config:** `lib/__tests__`, `lib/performance/__tests__`, `supabase/migrations/`, `.github/workflows/security-tests.yml`

EV-SDLC-TESTS

### Offline security smoke tests

```
$ npm run test:security-smoke  
  
> ai-studio-applet@0.1.0 test:security-smoke  
> npx tsx scripts/test-security-smoke.ts  
security-smoke: password policy  
security-smoke: privileged MFA roles include hr  
security-smoke: MFA policy function callable  
security-smoke: ops observability does not throw  
security-smoke: OK
```

Generated evidence card — FluxeHra ISO Alignment Pack

EV-SDLC-TESTS — Tests automatisés & preuves de changement (screenshot)

## EV-SECURITY-WATCH — Veille sécurité (CERT-FR / CISA / OSV)

- **Montrer:** Sanitized card: SU Admin Security Watch sources + daily GitHub Action + Dependabot — no operator emails
- **Tester:** Run `npm run security:watch`; open SU Admin → Security Watch; confirm daily `security-watch.yml` + Dependabot
- **Code / config:** `lib/security-watch.ts`, `app/api/su-admin/security-watch/route.ts`, `.github/workflows/security-watch.yml`; signed register (private) Certification documentation/policies/Security-community-subscriptions

EV-SECURITY-WATCH

Sanitized — no nominative PII

### Security Watch (CERT-FR / CISA / OSV)

```
ISO A.5.6 — contact with special interest groups
Product: SU Admin + Security Watch (impact-filtered RSS + lockfile)
CLI: npm run security:watch
CI: .github/workflows/security-watch.yml (daily) + Github Dependabot
Sources: CERT-FR avis, CISA KEV, OSV (npm lockfile)
Signed register (private): Security-community-subscriptions — 2026-08-14
Email backups: CERT-FR avis, CISA KEV, vendor status pages (no paid ISAC)
Public pack: no operator emails
```

FluxeHra ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SECURITY-WATCH — Veille sécurité (CERT-FR / CISA / OSV) (screenshot)

EV-ENV-SEPARATION — Séparation environnements Dev / production

- **Montrer:** Sanitized card: Git main→prod vs Git dev→Vercel saas-flex-hr-sql-dev + Supabase FluxeHRa-dev (eu-west-1) — no project API keys or full refs
- **Tester:** Confirm Vercel-dev Production deployment from dev ; Supabase FluxeHRa-dev Healthy in West EU; no customer PII in Dev
- **Code / config:** README.md deploy tracks; lib/non-prod-env-guard.ts ; private screenshots Certification documentation/ops/EV-ENV-SEPARATION-\*-2026-08-16.png

EV-ENV-SEPARATION

Sanitized — no nominative PII

Dev / production environment separation

```
ISO A.8.31 — separation of development, test and production
Production: Git main → Vercel saas-flex-hr-sql → Supabase FluxeHRa → fluxehra.ai
Dev: Git dev → Vercel saas-flex-hr-sql-dev → Supabase FluxeHRa-dev (eu-west-1 / West EU Ireland)
Evidence dated 2026-08-16: Vercel-dev Ready from branch dev; FluxeHRa-dev Healthy
Policy: Non-prod-data-policy (signed) — no customer PII dumps in Dev
Runtime: lib/non-prod-env-guard.ts (assertNonProdSupabaseUrl when PRODUCTION_SUPABASE_URL set)
Private full screenshots retained under Certification documentation/ops/
Public pack: no Supabase project refs / service keys
```

FluxeHRa ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-ENV-SEPARATION — Séparation environnements Dev / production (screenshot)

## EV-SIEM-AXIOM — Moniteurs SIEM Axiom (sécurité)

- **Montrer:** Sanitized dashboard card: fluxehra\_logs SECURITY\_EVENT monitors — BOLA/tenant, per-IP brute-force, high-signal (cron/RLS/HMAC/SSRF); no query payloads with PII
- **Tester:** Confirm three monitors + ingest smoke; private full screenshot retained by Foil Envie
- **Code / config:** lib/security-logger.ts, docs/siem-security-operations.md (internal), docs/subprocessors.md (Axiom)

EV-SIEM-AXIOM

Sanitized — no nominative PII

### Axiom security SIEM monitors

```
Dataset: fluxehra_logs (SECURITY_EVENT)
Monitors (3 slots): BOLA/tenant (403), per-IP brute-force, high-signal (cron/RLS/HMAC/SSRF)
Payload policy: no HR business PII in SIEM events
Edge: us-east-1.aws.edge.axiom.co (event storage/query)
Full operator screenshot: retained privately by Foil Envie (Aug 2026 rev. 6)
Annex A: A.8.15 Logging (Implemented) · A.8.16 Monitoring (Implemented – not a 24x7 outsourced SOC)
```

FluxeHra ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SIEM-AXIOM — Moniteurs SIEM Axiom (sécurité) (screenshot)

EV-SUPPLIER-VERCEL — Assurance fournisseur Vercel (synthèse)

- **Montrer:** Sanitized evidence card: certificate/attestation on file (Jul 2026) — no account secrets
- **Tester:** Annual re-review; align with Trust Center hosting regions
- **Code / config:** Provider file (private); `vercel.json` region `dub1`

EV-SUPPLIER-VERCEL

Sanitized — no nominative PII

Vercel supplier assurance

Supplier: Vercel Inc. (application hosting / Edge)  
Evidence on file (private): supplier certificate / attestation - dated 28 Jul 2026  
Product alignment: `vercel.json` region `dub1` (Dublin)  
Customer-facing note: see Trust Center /trust - Hosting & sub-processors  
Cadence: re-review annually; watch `status.vercel.com` for changes  
Annex A: A.5.19 / A.5.21 / A.5.22 Implemented · A.5.20 Partial (customer DPA)

FluxeHra ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SUPPLIER-VERCEL — Assurance fournisseur Vercel (synthèse) (screenshot)

EV-SUPPLIER-SUPABASE — Assurance fournisseur Supabase (synthèse)

- **Montrer:** Sanitized evidence card: certificate/attestation on file (Jul 2026) — region eu-west-1
- **Tester:** Annual re-review; document backup plan RPO/RTO in Provider ISMS
- **Code / config:** Provider file (private); Trust Center hosting section

EV-SUPPLIER-SUPABASE

Sanitized — no nominative PII

Supabase supplier assurance

Supplier: Supabase (PostgreSQL, Auth, Storage)  
Evidence on file (private): supplier certificate / attestation – dated 28 Jul 2026  
Production region documented: eu-west-1 (Ireland)  
Backup / RPO-RTO: document targets in Provider ISMS from Supabase plan  
Annex A: A.5.19 / A.5.21 / A.5.22 / A.5.30 Implemented · A.5.20 Partial (customer DPA)

FluxeHRa ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SUPPLIER-SUPABASE — Assurance fournisseur Supabase (synthèse) (screenshot)

EV-SUPPLIER-CURSOR — Assurance fournisseur Cursor / Anysphere (synthèse)

- **Montrer:** Sanitized card: SOC 2 Type II + security program / NDA on file for development tooling
- **Tester:** Does not replace FluxeHRa pen-test; keep tool assurance separate from product SoA
- **Code / config:** Provider file (private)

EV-SUPPLIER-CURSOR

Sanitized — no nominative PII

Cursor / Anysphere tooling assurance

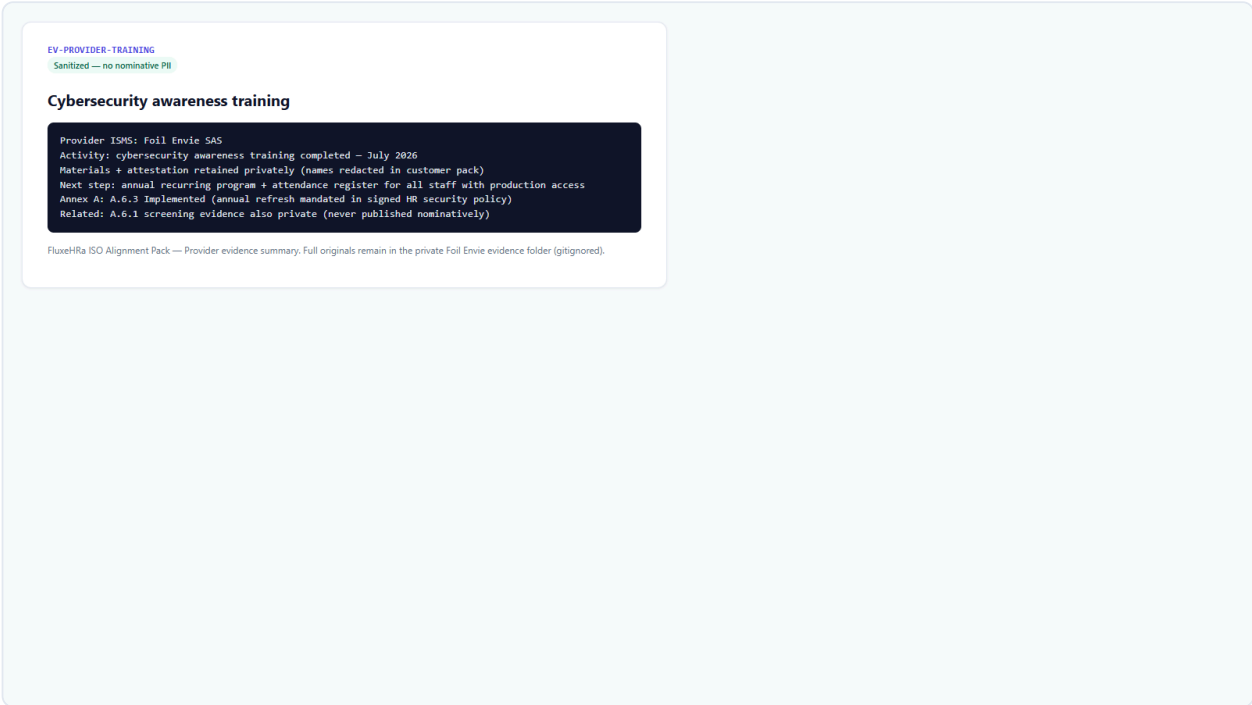
Supplier: Anysphere (Cursor) — development tooling (not a FluxeHRa runtime sub-processor for HR PII)  
Evidence on file (private): SOC 2 Type II (2025), security program update, pen-test executive summary, NDA  
Scope note: tool assurance ≠ FluxeHRa product pen-test or ISO certificate  
Annex A: A.5.19 / A.5.21 / A.6.6 Implemented · A.5.35 Partial (Independent FluxeHRa ISMS review)

FluxeHRa ISO Alignment Pack — Provider evidence summary. Full originals remain in the private Foil Envie evidence folder (gitignored).

EV-SUPPLIER-CURSOR — Assurance fournisseur Cursor / Anysphere (synthèse) (screenshot)

EV-PROVIDER-TRAINING — Formation sensibilisation cybersécurité (Provider)

- **Montrer:** Sanitized card: training completed Jul 2026 — no personal names in customer pack
- **Tester:** Retain full attestation privately; extend to annual all-staff program
- **Code / config:** Provider ISMS (private folder)



EV-PROVIDER-TRAINING — Formation sensibilisation cybersécurité (Provider) (screenshot)

[↑ Sommaire](#) · [↑ Languages](#)

## 11. Modèle de responsabilité partagée (ISO 27017)

**Client (Responsable de traitement)**

Politiques, DPIA, DPA, base légale, cycle de vie utilisateurs & revues d'accès, instructions de rétention, décisions DSAR

↓ instruct / configure

**FluxeHRa (Sous-traitant — Application)**

RBAC, RLS, MFA, audit, chiffrement, visibilité, processus RH, contrôles d'intégration

↓ opéré par

**Foil Envie SAS (SMSI éditeur)**

Politiques corporate, sécurité RH, locaux, programme fournisseurs, exercices IR, DdA / registre des risques (signés août 2026 — §3 les cartographie en **Implémenté** ; compteur **SMSI éditeur (Foil Envie)** = 0)

↓ s'exécute sur

### Sous-traitants techniques

Supabase (PostgreSQL, Auth, Storage — eu-west-1) · Vercel (app/API — dub1) · Axiom (SIEM sécurité — edge US East)

Enregistrer régions et contrats des sous-traitants dans le registre de traitements.

[↑ Sommaire](#) · [↑ Languages](#)

## 12. Recommandations — plus auditable & rassurant

1. **DPA client signé** (A.5.20 / A.5.31) — finaliser `public/legal/dpa*.md` avec le premier client commercial (suivi déjà signé).
2. **Revue indépendante SMSI** (A.5.35) — audit externe ou campagne ISO quand budgété.
3. **Exercice restore** — sous 30 j après activation Supabase Pro (A.5.30 déjà Implemented avec engagement).
4. **Optionnel** : APM Sentry ; E2E IDOR navigateur ; `PRODUCTION_SUPABASE_URL` sur Preview/Dev Vercel pour durcir la garde non-prod.

[↑ Sommaire](#) · [↑ Languages](#)

## 13. Écarts connus (synthèse honnête)

- Aucune *certification* ISO / SOC revendiquée par le produit (processus d'entreprise).
- Artefacts SMSI Provider (juil.–août 2026) : certificats fournisseurs, formation, screening, pack IR/Backup/NDA Wave A/B **signés**, plus pack maximize **signé** (2026-08-13) : gouvernance, usage acceptable, classification/cloud, secrets staff, physique home-office, cycle de vie RH, signalement/preuves, rétention, actifs/config, endpoints, audit/IP, Secure-development-pack — privés sous `Certification documentation/`. Annexe A mise à jour Implemented là où la preuve est complète.
- Peu de lignes Annexe A restent ouvertes : A.5.20 / A.5.31 (DPA client), A.5.35 (revue indépendante). A.5.6 clos — voir `EV-SECURITY-WATCH` (Security Watch + abonnements signés). A.8.23 clos (filtrage N/A compensé).
- Analyse/purge de rétention implémentées côté serveur.
- Export DSAR portable + anonymisation in-place (prise en compte legal hold).
- MFA pour rôles privilégiés (admin / super\_admin / hr / Domain Admin) **ON** par défaut en production.
- Embauche / māj / sortie Core HR journalisées.
- UI / e-mails de définition et réinitialisation du mot de passe affichent la règle  $\geq 20$  + complexité ; les mots de passe existants restent valides jusqu'au changement.
- Trust Center `/trust` ; contact vulnérabilités `contact@fluxehra.ai` ; `SECURITY.md`, IR, sauvegarde/restauration, sous-traitants, pack AIPD.
- Export preuves de conformité JSON ; `npm run test:security-smoke`, `test:security-idor`, workflow GitHub `security-tests`.
- Écarts honnêtes restants : APM Sentry optionnel ; **DPA client** (A.5.20/A.5.31) ; **revue indépendante** (A.5.35) ; restore drill après Pro. A.5.6 clos via `EV-SECURITY-WATCH`. A.8.23 clos via filtrage web N/A compensé.
- Écrans d'évidence UI authentifiés peuvent encore être des placeholders jusqu'à capture sur org démo — voir `docs/iso-demo-session-capture-guide.md`.

Ce pack reflète l'état de l'application à la génération. Contact : `contact@fluxehra.ai`

