Security vulnerability disclosure

FluxeHRa welcomes responsible disclosure of security issues in the product and infrastructure we operate.

How to report

Email **contact@fluxehra.ai** with:

- A clear description of the issue and affected URL/API
- Steps to reproduce (PoC without weaponized exploit payloads)
- Impact assessment (confidentiality, integrity, availability)
- Your contact details for follow-up

Please do **not** publicly disclose the issue until we have confirmed a fix or agreed a disclosure date.

Scope

In scope: `https://fluxehra.ai`, authenticated application APIs, multi-tenant isolation bugs, authentication/MFA bypasses, unauthorized access to other organizations' data, and forgery of optional integration webhooks (e.g. DocuSign Connect without valid HMAC, cross-tenant envelope completion).

Out of scope: social engineering of FluxeHRa staff, physical attacks, DoS volume testing without prior approval, and issues solely in third-party products (Supabase, Vercel, DocuSign) that are already publicly documented — we still appreciate a heads-up if they affect our tenants.

Response targets

- Acknowledgement within **3 business days**
- Initial severity triage within **10 business days**
- Coordinated fix timeline communicated based on severity

Thank you for helping keep customer HR data safe.