

AXS Passport Security



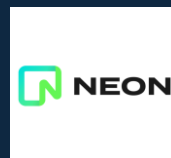
Empowering Inclusive Workplaces with Secure, User-Centric Accessibility

- As a revolutionary digital tool for sharing workplace adjustments and inclusion needs, AXS Passport puts control in the hands of individuals - whether neurodiverse, disabled, or anyone seeking a more inclusive environment.
- Hosted on Vercel's cutting-edge platform, our security architecture ensures your sensitive data is protected at every step, from creation to sharing.
- We handle personal accessibility data with the utmost care, complying with global standards like ISO-27001:2022, GDPR and leveraging enterprise-grade, zero-knowledge infrastructure.
- Vercel's customers include; Airbnb, eBay, PayPal, Uber, NetFlix, TicketMaster, EventBrite, GitHub, Nike and Marvel.

Vercel is compliant with;



Our
Partners:



AXS Passport Security



Compliance & Auditing

- ISO 27001:2022 Certified Infrastructure: Vercel's platform ensures our hosting meets international security standards for Information Security Management Systems (ISMS).
- GDPR & Privacy Compliance: As a UK-based tool (supported by government since 2021), we align with data protection laws; Vercel's underlying providers (AWS, Azure, GCP) add ISO 27017/18/27701 support.
- Audit Logs & Monitoring: Real-time logs via Vercel Analytics, integrated with tools like Datadog for tamper-proof auditing. Enterprise clients get custom reports.

Data Encryption & Storage

- End-to-End Encryption: All data in transit uses HTTPS with automatic SSL certificates; at rest, it's encrypted via Vercel's integrations (e.g., AWS S3-like storage).
- Secure Databases: Tenant-isolated storage using compliant services like Vercel Postgres or Supabase, with row-level security to prevent cross-user leaks.
- Vercel KV/Edge Config: Fast, encrypted key-value stores for configs and flags, accessible globally without performance hits.

AXS Passport Security

Global Edge Network & DDoS Protection



- Vercel Firewall: Always-on, multi-layer Web Application Firewall (WAF) blocks billions of attacks weekly, including L3/L4 volumetric floods and L7 HTTP bots.
- Anycast Routing: Traffic is routed to the nearest of 30+ Points of Presence (PoPs) worldwide, mitigating DDoS attempts before they reach your site.
- BotID & Challenge Mode: Invisible bot detection and lightweight challenges filter malicious traffic without disrupting legitimate users.
- Benefit for Clients: 99.99%+ uptime ensures seamless access for employees sharing passports, even under attack.

AXS Passport Security

Authentication & Authorization



- Multi-Factor Authentication (MFA): Secure logins via email verification, SMS passcodes, or app-based one-time codes, integrated with providers like Auth0 or Clerk.
- Edge Middleware: Runs at Vercel's edge to validate JWTs, tenant IDs, and roles in milliseconds, enforcing access before requests hit the backend.
- Role-Based Access Control (RBAC): Users control who sees their passport (e.g., HR only, full team)—preventing unauthorized views.
- Tokenization: Sensitive data (e.g., adjustment details) is tokenized for storage and transit.

Security Layer	Vercel Feature
Network	Global PoPs + Firewall
Identity	Edge Middleware + MFA
Data	Encrypted Storage + KV
Compliance	ISO 27001 + GDPR Tools