giveeasy

GiveEasy Security, Infrastructure & Compliance Overview

1. Overview

This document outlines GiveEasy's approach to cybersecurity, hosting infrastructure, data resilience, and compliance alignment. It is intended to support IT due diligence, vendor assessments, and risk management reviews.

---

2. Cybersecurity Practices

GiveEasy applies the following technical and organisational measures to ensure secure operations:

- ***PCI Compliance:*** We are PCI-compliant through our integration with Stripe and PayPal. We do not store, transmit, or access raw credit card data.
- ***Data Encryption:*** All data is encrypted in transit (TLS 1.2+) and at rest (AES-256) using native AWS encryption capabilities.
- ***Access Control:***
    - Role-based access control (RBAC) enforced across services.
    - Multi-factor authentication (MFA) is required for all admin-level access.
- ***Internal Security Testing:*** Regular internal penetration testing is performed on both applications and infrastructure.
- ***Staff Vetting & Training:*** All staff and contractors:
    - Undergo reference checks (minimum 5 years history).
    - Are trained on secure data handling and breach response.
    - Must use encrypted channels (SFTP or similar) for file transfers.

---

3. Real-Time Monitoring & Threat Detection

We employ the following tools and practices to detect and prevent security threats:

- ***Datadog:*** Real-time session monitoring, anomaly detection, alerting.
- ***AWS WAF:*** Layer 7 firewall, IP/geolocation-based filtering, bot protection.
- ***AWS CloudWatch:*** Centralised logging and metric monitoring for infrastructure and application-level events.
- ***Stripe Radar:*** AI-powered fraud detection for donation transactions.
- **Vercel Firewall** – Built-in, always-on distributed mitigation of L3/L4/L7 attacks, including TCP floods and SYN/DDoS storms. Protection is enabled by default on all Vercel plans.

---

4. Hosting Infrastructure

Our infrastructure is cloud-native and fully managed for high availability:

- ***Hosting Providers:*** We use AWS (Sydney Region) and Vercel for all hosting and content delivery.
- ***Services Used:*** AWS Lambda, DynamoDB, S3, RDS (PostgreSQL), CloudFront.
- ***Data Residency:***
    - Donor and operational data is stored in the *AWS Sydney region* (ap-southeast-2).
    - Login credentials are stored in *Auth0's EU region* to support GDPR compliance for global users.

---

5. Redundancy & Failover

GiveEasy's public donation infrastructure is designed for resilience:

- ***Stateless Architecture:*** Donation flows are stateless, serverless, and distributed — removing single points of failure.
- ***Multi-AZ Redundancy:*** All core AWS services are deployed across multiple availability zones (AZs).
- ***CDN Edge Distribution:*** Vercel automatically caches and delivers pages globally.
- ***Payment Gateway Recovery:*** Stripe and PayPal act as the source of truth for all financial data and enable full recovery if needed.

---

6. Disaster Recovery & Business Continuity

Disaster recovery and business continuity practices include:

- ***Nightly Backups:*** Admin platform databases (PostgreSQL) are backed up nightly and stored securely.
- ***RTO:*** ≤ 2 hours for critical infrastructure.
- ***RPO:*** ≤ 24 hours for admin platform data.
- ***Testing & Review:*** DR processes are reviewed and tested quarterly.

---

7. Hosting Agreements & Back-to-Back SLAs

GiveEasy relies on the following providers with their own SLAs and compliance guarantees:

- ***AWS:***
  - 99.99% uptime SLA across core services (Lambda, S3, RDS).
  - Compliance certifications include PCI-DSS, ISO 27001, SOC 1/2/3, GDPR, HIPAA, FedRAMP, and more.
- ***Vercel:***
  - Edge CDN with 99.9% SLA and automatic failover.
- ***Back-to-Back SLA Position:***
  GiveEasy's infrastructure is architected using best-in-class providers (AWS, Vercel, Stripe), and we propagate their operational reliability, availability guarantees, and monitoring capabilities throughout our platform.
  We actively monitor all upstream service SLAs and maintain continuous oversight via dashboards and alerts to ensure consistent service for our clients.

---

giveeasy

8. Compliance Summary

Area	Status
PCI DSS	✅ (via Stripe/PayPal integration – no card data stored by GiveEasy)
GDPR	✅ (through use of Auth0 EU region and privacy-aligned data handling)
Australian Privacy Principles (APP)	✅ (see GiveEasy Privacy & Data Policy)
ISO / SOC Certifications	❌ Not currently certified independently (rely on AWS/Stripe certs)

---

9. Contact

For questions related to security, infrastructure, or compliance, please contact:
GiveEasy Technical Team
support@giveeasy.org