Security Whitepaper

Introduction:

Easocare provides a mobile app to thousands of users in India to help digitize healthcare and store medical records securely. Security is a key component in our offerings, and is reflected in our people, process, and products. This page covers topics like cloud security, application security, and HR security to explain how we offer security to our customers.

Cloud security

Data Center Physical Security

- **Facilites**:

  Easocare hosts Service Data primarily in AWS data centers that have been certified as ISO 27001, PCI DSS Service Provider Level 1, and/or SOC 2 compliant. **Learn more about Compliance at AWS.**
  AWS infrastructure services include backup power, HVAC systems, and fire suppression equipment to help protect servers and ultimately your data. **Learn more about Data Center Controls at AWS.**

- **On-Site Security:**

  AWS on-site security includes a number of features such as security guards, fencing, security feeds, intrusion detection technology, and other security measures. **Learn more about AWS physical security.**

Network Security

- **Protection**:

  Our network is protected through the use of key AWS security services, integration with our Cloudflare edge protection networks, regular audits, and network intelligence technologies, which monitor and/or block known malicious traffic and network attacks.

- **Architecture**:

  Our network security architecture consists of multiple security zones. More sensitive systems, like database servers, are protected in our most trusted zones.

Other systems are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the Internet, and internally between the different zones of trust.

- **Network Vulnerability Scanning:**

  Network security scanning gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems.

- **Intrusion Detection and Prevention:**

  Service ingress and egress points are instrumented and monitored to detect anomalous behavior. These systems are configured to generate alerts when incidents and values exceed predetermined thresholds and use regularly updated signatures based on new threats. This includes 24/7 system monitoring.

- **DDoS Mitigation:**

  Easocare has architected a multi-layer approach to DDoS mitigation. A core technology partnership with Cloudflare provides network edge defenses, while the use of AWS scaling and protection tools provide deeper protection along with our use of AWS DDoS specific services.

Encryption

- **Encryption in Transit:**

  All communications with Easocare UI and APIs are encrypted via industry standard HTTPS/TLS (TLS 1.2 or higher) over public networks. This ensures that all traffic between you and Easocare is secure during transit. Additionally for email, our product leverages opportunistic TLS by default. Transport Layer Security (TLS) encrypts and delivers email securely, mitigating eavesdropping between mail servers where peer services support this protocol. Exceptions for encryption may include any use of in-product SMS functionality, any other third-party app, integration, or service subscribers may choose to leverage at their own discretion.

- **Encryption at Rest:**

  Service Data is encrypted at rest in AWS using AES-256 key encryption.

Availability & Continuity

- **Uptime**:

  Easocare maintains a publicly available **system-status webpage**, which includes system availability details, scheduled maintenance, service incident history, and relevant security events.

Application Security

Secure Development (SDLC)

- **Secure Code Training:**

  At least annually, engineers participate in secure code training covering **OWASP Top 10** security risks, common attack vectors, and Easocare security controls.

- **Framework Security Controls:**

  Easocare leverages modern and secure open-source frameworks with security controls to limit exposure to OWASP Top 10 security risks. These inherent controls reduce our exposure to SQL Injection (SQLi), Cross Site Scripting (XSS), and Cross Site Request Forgery (CSRF), among others.

- **Separate Environments:**

  Testing and staging environments are logically separated from the Production environment. No Service Data is used in our development or test environments.

Vulnerability Management

- **Static Code Analysis:**

  The source code repositories for both our platform and mobile applications are scanned for security issues via our integrated static analysis tooling.

- **Dynamic Vulnerability Scanning:**

  We continuously and dynamically scan our core applications against the OWASP Top 10 security risks. We have engineering teams to remediate any discovered issues.

Human Resources Security

Security Awareness

- **Policies**:

  Easocare has developed a comprehensive set of security policies covering a range of topics. These policies are shared with and made available to all employees and contractors with access to Easocare information assets.

- **Training**:

  All employees attend a Security Awareness Training, which is given upon hire and annually thereafter. All engineers receive annual Secure Code Training. The Security team provides additional security awareness updates via email and blog posts

Employee Vetting

- **Background Checks:**

  Easocare performs background checks on all new employees in accordance with Indian laws. These checks are also required to be completed for contractors. The background check includes criminal, education, and employment verification. Interns are included.

- **Confidentiality Agreements:**

  All new hires are required to sign Non-Disclosure and Confidentiality agreements. Interns included.

Notice:

All notices of Company will be served by email or by general notification on the Website. Any notice provided to Company pursuant to the Terms should be sent to support@easocare.com You cannot assign or otherwise transfer the Terms, or any rights granted hereunder to any third party. Company's rights under the Terms are freely transferable by Company to any third parties without the requirement of seeking Your consent. If, for any reason, a court of competent jurisdiction finds any provision of these Terms, or portion thereof, to be unenforceable, that provision shall be enforced to the maximum extent permissible so as to give effect to the intent of the parties as reflected by that provision, and the remainder of the Terms shall continue in full force and effect. Any failure by Company to enforce or exercise any provision of the Terms, or any related right, shall not constitute a waiver by Company of that provision or right.