Security Policy

Objective:

The goals of this Security Policy document are to help ensure that all products, solutions, and infrastructure are designed, developed, and maintained with security in mind.

Scope:

The scope of this document includes all software developed and infrastructure maintained by Deeloh Technologies, Inc.

Methodology:

We are committed to the confidentiality, integrity, and availability of our customer information and believe that the foundation of a highly secure system is that the security is built into the software from the initial stages of its concept, design, development, deployment, and beyond. Security principles are applied to all stages of the development lifecycle.

With a goal to incorporate security at the earliest possible phase of the SDLC, we incorporate specific application security requirements during the concept/design phases of the product.

Our methodology for ensuring application security is based largely on OWASP Best Practices. We follow *OWASP Secure Coding Practices* and reference the *OWASP Top 10* to assess risk and prioritize security related items.

Training and Awareness:

Development and QA Teams attend training sessions to ensure secure coding best practices are utilized and a deep understanding of what each vulnerability means. We believe that the answer to the question 'why' is just as important as the 'how' when remediations are implemented for security flaws or vulnerabilities.

The following are just a few of the training resources that we utilize for security training:

- OWASP Developer Secure Coding Best Practices
- OWASP Top 10
- OWASP Security Cheat Sheets
- Microsoft Security Best Practices
- Security Webinars

SDLC and Security:

We employ the following security tools and techniques in our SDLC life cycle. This allows us to provide several security 'gates' ensuring a secure SDLC.

- Very early in our SDLC, in our requirements and design phases, we perform impact and risk analysis with security in mind.

- In Development, we utilize a Visual Studio Extension, Security Code Scan, to enable developers to find and fix vulnerabilities early during the development process. https://security-code-scan.github.io/.
- When Development is complete, we perform security code reviews in addition to our standard code reviews.
- Once our application is ready for testing, our QA team tests security in addition to application functionality.
- All findings are prioritized based on risk and the OWASP Top 10 to determine order of remediation.

Access Control:

- All servers are in a private subnet accessible only by Secure VPN or the AWS Console. IAM Roles ensure that the principle of least privilege is utilized.
- AWS SSO is utilized with Multi-Factor Authentication for an extra layer of security.
- Monitoring and Auditing of Login Attempts.

Data Security/Confidentiality:

- Data stored at rest is encrypted using AES-256 encryption..
- All data in transit is encrypted using secure protocols.
- All data backups are encrypted and stored securely.

Availability/Disaster Recovery:

- Multiple AWS availability zones and load balancers.
- Monitoring for key resource metrics and proactive notification if thresholds are exceeded facilitating reliability, availability, and performance.
- Frequent server and database backups are performed.
- Secondary AWS Region Disaster Recovery Infrastructure in the event of a primary region outage.

System Hardening:

- All root accounts and database admin accounts are disabled. Dedicated accounts are utilized based on role and least privilege.
- All servers are patched frequently with the latest updates. Critical security patches are expedited.
- Antivirus is installed and updated on all servers.