mission™

LET'S ACHIEVE YOURS

Mission Security Management

About Us

COMPANY BACKGROUND

Mission Cloud Services, Inc. ("Mission"), is an AWS Premier Consulting Partner, formed by the 2018 merger of Reliam, Stratalux, and G2 Tech Group, three companies united by their shared commitment to helping their clients harness the power of the cloud to fuel innovation and drive the growth of their businesses.

EXECUTIVE SUMMARY

Mission takes its responsibilities seriously for protecting the confidentiality, integrity, and availability of data. Mission utilizes **Industry Best Practices** to protect all confidential information for which it is responsible.

Mission has implemented a **Security Management Program** in order to establish comprehensive real-world security. Mission verifies the effectiveness of their **Security Program** with **Compliance reviews and audits**, conducted both internally, and externally by certified independent third-party organizations.

INDUSTRY COMPLIANCE

Mission verifies the effectiveness of its security program with the following **Compliance Initiatives**:

- **AWS MSP Partner Program Audit**
  Mission undergoes a complete audit of all requirements for the AWS MSP Partner Program every 24 months.
- **Annual SOC 2, Type 2 Audit**
  Mission annually engages a Third Party firm to conduct a SOC 2 Audit, and issue a SOC 2, Type 2 Report.
- **Annual ISO-27001 Audit**
  Mission annually engages a Third Party firm to conduct an Audit of its Information Security Management System (ISMS), in accordance with the ISO-27001+ series.
- **Annual HIPAA Review**
  Mission performs periodic reviews of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule requirements, and applicable trust services criteria set forth in TSP section 100A.
- **NYDFS Cybersecurity Regulation**
  Mission works to ensure that it's systems, where applicable, comply with the New York Department of Financial Services (NYDFS) Cybersecurity Regulations.
- **AWS Competency Audits**
  Mission is audited periodically for the following AWS Competencies: Healthcare, Life Sciences, Microsoft Workloads, Migrations, and DevOps.
- **AWS Solution Provider Program**
  Mission conforms with all requirements necessary to function as an AWS Solution Provider.

Our Services

MISSION'S SECURITY MANAGEMENT PROGRAM

Mission has established a **Security Management Team** to create and enforce the **Security Management Program**, as defined by **Mission's Security Policies and Procedures**.

Our **Security Management Team** is responsible for overseeing known incidents, patch levels, vulnerability assessments, **Penetration Tests**, **Risk Assessments**, policy review, and policy enforcement.

The following is a summary of Mission's security practices, as implemented by out **Security Management Team**:

Access Control (Network, Application, Infrastructure)

- Role-based access has been implemented, with fully unique user credentials, to limit access on an as-needed basis for all digital assets. SAML authentication is implemented whenever applicable.
- Access to infrastructure, and administrative functions is restricted to a minimum necessary for regular business.
- User access is reviewed periodically.
- User access is discontinued upon employee termination.
- Default credentials are changed, and given values consistent with administrative credential requirements.
- Multi-factor authentication and encrypted channels are used for all administrative account access.
- **Strong Password** complexity rules are thoroughly enforced.

Risk Management

- **Risk Assessments** are performed to ensure compliance with the requirements and commitments of SOC 2 and ISO-27001.
- Ongoing risk assessment is implemented in the form of regular oversight meetings, event log monitoring and response, regular vulnerability assessments.
- Regular policy and procedure audits are reviewed and updated to reflect the changing threat landscape.

Third Party Risk Management

- A **Third-party Security Policy** is established and enforced to ensure requirements are followed, such as by vendors.

Our Services
(CONT.)

Change Management/Systems and Software Development

- A formalized change management process has been implemented to: record changes, assess the security risk of changes, approve changes, and test changes.
- **Static Code Analysis** shall be used to assess any custom software for security vulnerabilities prior to code commits.
- Mission maintains security-hardened images and configuration templates for authorized operating systems and software.
- Any database, infrastructure, application code, or CRM changes shall be tested prior to production implementation.
- Standardized server builds are utilized to enhance security.
- **Patch Management** is implemented in accordance with established policies.

Asset Management

- All **Asset classes** (devices, appliances, etc.) are subject to asset tracking and inventory. **Asset Numbers** are assigned to each item, and are tracked in a central database.

Incident Management and Monitoring

- The **Security Management Team** is responsible for monitoring known incidents, patch levels, vulnerability assessments, penetration tests, policy and procedure reviews, and enforcement thereof.
- Changes to policy and procedures are implemented, as needed, in response to any incidents.
- Employees are instructed to report potential security incidents to the Security Management Team.
- Various security utilities are used to identify and detect potential threats and incidents. These include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs.
- Logging is enabled within the AWS environment and includes information, such as an event source, date, user, timestamp, source addresses, destination addresses, and other elements. Log analytic tools are deployed systematically and manually to identify anomalies or abnormal events.
- Incidents are tracked using an internal task tool and monitored until resolved.

Business Continuity and Disaster Recovery

- Hosted databases are backed up.
- **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO)** are defined for Mission services, including a business impact assessment.
- **Crisis Communication Team** roles have been defined.
- Testing of the business continuity and disaster recovery plan are scheduled annually.

Our Services
(CONT.)

Personnel Security

- Background checks are performed on new employees, who are also required to review and acknowledge their receipt of relevant security policies.
- New employees are subject to Mission's procedures for accessing systems and sanctions for violating Mission's information security policy.
- Employees are instructed to report potential security incidents to the Information Compliance and Security function.

Vulnerability Management and Penetration Testing

- **Penetration Tests** and **Vulnerability Assessments** are performed at least annually.
- Software tools shall be used within the SDLC to help ensure vulnerabilities in code are identified and remediated before release.

Physical and Environmental Security

- All computer facilities and access thereto are controlled at AWS data centers.
- Extensive physical security is in place to help ensure the security and integrity of relevant facilities.

Security Awareness and Training

- During annual security training and awareness programs, management ensures communication of the latest security policies, as well as the importance of data privacy at Mission.
- Any software development personnel receive training in writing secure code for their specific development environment and responsibilities.
- Regularly scheduled **Phishing assessments** are performed over email and phone to ensure Mission engineers are properly validating the identity of the support requestor.

Customer Data Privacy

- Information assets are assigned a sensitivity level, which guides the selection of protective measures, such as encryption, to secure the information.

Endpoint Management

- Endpoint management solutions are established for company-issued devices.
- Policy enforcement ensures encryption for data-at-rest, remote-wipe, and anti-malware.