MARK43

# Mark43 Information Security Program

Mark43's mission is to empower communities and their governments with new technologies that improve the safety and quality of life for all. Information security is vital to this mission in order to ensure the confidentiality, integrity, and availability of customer's data within the Mark43 Public Safety Platform Software-as-a-Service (SaaS) offering.

## Risk Management and Compliance

Mark43 has developed and implemented an information security risk management and compliance program based on industry best practices including National Institute of Standards and Technology (NIST), Criminal Justice Information Service (CJIS) Security Policy, and American Institute of CPAs (AICPA) trust services criteria. Mark43 engages, annually, with a third-party auditing firm to perform a SOC 2 audit of the company's security, availability, and confidentiality practices.

## Vulnerability Management

Mark43 maintains a comprehensive security assessment and testing strategy to identify vulnerabilities and weaknesses. This includes both internal and external third-party assessments to validate the effectiveness of the platform's security controls. Regular vulnerability scans and penetration testing are conducted of the platform cloud infrastructure as well as the application leveraging industry standard vulnerability scanning tools. In addition, Mark43 operates a vulnerability disclosure and bug bounty program to allow security researchers to report potential security issues they may have identified.

## Data Security

Mark43 has implemented data security controls to protect the confidentiality of customer data. All data to and from the Mark43 platform is encrypted utilizing industry-standard FIPS 140-2 encryption. Additionally, customer data within the platform database is encrypted at rest.

## Cloud Security and Resiliency

The Mark43 platform is built with a secure and resilient architecture leveraging tools of the underlying Infrastructure-as-a-Service (IaaS) provider to scale and meet demand. IaaS cloud computing resources are housed in highly available data center facilities. Mark43 is hosted within regions that distribute multiple data centers across geographically unique availability zones to ensure high availability and redundancy for intra-region disaster recovery and business continuity processes.

Security controls are in place to monitor and control communications at the external boundary of the system and at key internal boundaries. These include firewalls, web application firewalls, load balancers, network security groups, and subnets. The security of the environment is monitored utilizing security posture management, threat prevention, and intelligent threat detection tools.

### Incident Response

Mark43 has a documented Incident Response Program (IRP), including procedures to be taken in response to information security incidents. Mark43 will notify impacted customers in the event Mark43 reasonably believes that there has been any unauthorized access, acquisition, disclosure, use, modification, loss, or destruction of customer data. Mark43 will promptly investigate the security incident, take necessary steps to eliminate or contain the exposure of customer data, and will keep the customer informed of the status of the security incident.

### Change Management

Changes to the Mark43 codebase and infrastructure are deployed to a QA environment where changes are tested and systems are monitored to ensure that changes do not result in a loss of security, system functionality, stability, or performance. Changes to the code run through a set of automated unit tests and only builds passing all tests are deployed to the QA environment. Once tests are validated in QA, validated builds are able to be pushed to the staging environment. Once in the staging environment, another set of tests are conducted. Only validated builds from the staging environment are deployed to the production environment.

### Personnel Security

Mark43 maintains rigorous personnel security procedures to ensure that all employees are appropriately vetted. All employees are subject to corporate-level background checks as a standard hiring practice. Employees with admin access to the system are screened at the highest risk designation level, which includes a pre-employment background check, CJIS background check (FD-258 Fingerprint cards, CJIS Security Addendum, and CJIS Level 4 Training), as well as a Federal fingerprint-based background check.

Mark43 maintains a holistic security awareness and training program which consists of regular review and attestation of security policies, data security and privacy video training, role specific training, and CJIS Level 4 training.