Configuration Management Policy

Marketware, Inc. standardizes and automates configuration management through the use of SQL scripts as well as documentation of all changes to production systems and networks. SQL Scripts automatically configures all Marketware, Inc. systems according to established and tested policies, and is used as part of our Disaster Recovery plan and process.

Applicable Standards from the HITRUST Common Security Framework

- 06 - Configuration Management

Applicable Standards from the HIPAA Security Rule

- 164.310(a)(2)(iii) Access Control & Validation Procedures

Configuration Management

- SQL is used to standardize and automate configuration management.
- OSSEC is used to scan systems every 2 hours and on reboot. These scans capture file system changes and also unauthorized or malicious software.
- No systems are deployed into Marketware, Inc. environments without approval of the Marketware, Inc. CSO.
- All changes to production systems, network devices, and firewalls are approved by the Marketware, Inc. CSO before they are implemented to assure they comply with business and security requirements. Additionally, all changes are tested before they are implemented in production. All changes are documented using Visual Studio Team Services. Implementation of approved changes are only performed by authorized personnel.
- An up-to-date inventory of systems is maintained using Excel spreadsheets and architecture diagrams created in Lucid Chart are hosted on Dropbox. All systems are categorized as production and utility to differentiate based on criticality.
- Clocks are synchronized across all systems using NTP. Modifying time data on systems is restricted.
- All front end functionality (developer dashboards and portals) is separated from backend (database and app servers) systems by being deployed on separate servers.
- All software and systems are tested using unit tests and end to end tests.
- All committed code is reviewed via Code Reviews to assure software code quality and proactively detect potential security issues in development.

- Marketware, Inc. utilizes development and staging environments that mirror production to assure proper function.
- Marketware, Inc. also deploys environments locally to assure functionality before moving to staging or production.
- Marketware, Inc. schedules production deployments roughly every four weeks.
- All formal change requests require unique ID and authentication.
- ClamAV is run on all production hosts for anti-virus protection. Hosts are scanned daily for malicious binaries in critical system paths. The malware signature database is checked hourly and automatically updated if new signatures are available.
- All physical media is encrypted at provisioning. To verify encryption is consistent and in place for all production storage, checks are performed on a quarterly basis.