Data Intergrity Policy

Marketware, Inc. takes data integrity very seriously. As stewards and partners of Marketware, Inc. Customers, we strive to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical settings in support of the Marketware, Inc. mission of data protection.

Applicable Standards from the HITRUST Common Security Framework

- 10.b - Input Data Validation

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(8) – Evaluation

Data integrity Policy

- Production Systems that create, receive, store, or transmit customer data (hereafter "Production Systems") must follow the following guidelines.

Disabling non-essential services

- All Production Systems must disable services that are not required to achieve the business purpose or function of the system.

Monitoring Log-in Attempts

- All access to Production Systems must be logged. This is done following the Marketware, Inc. Auditing Policy.

Prevention of malware on Production Systems

- All Production Systems must have OSSEC running at set to scan system every 2 hours and at reboot to assure not malware is present. Detected malware is evaluated and removed.
- All Production Systems are to only be used for Marketware, Inc. business needs.

Patch Management

- Patches, application, and system OS versions are kept up to date at all times. New versions are tested.
- Administrators subscribe to mailing lists to assure up to date on current version of all Marketware, Inc. managed software on Production Systems.

Intrusion Detection and Vulnerability Scanning

- Production Systems are monitors using IDS systems. Suspicious activity is logged and alerts are generated.

- Vulnerability scanning of Production Systems must occur on a predetermined, regular basis, no less than annually. Currently it is weekly. Scans are reviewed by Security Officer, with defined steps for risk mitigation, and retained for future reference.

Production System Security

- System, network, and server security is managed and maintained by the VP of Business Intelligence and the Security Officer.
- Up to date system lists and architecture diagrams are kept for all Production environments.
- Access to Production Systems is controlled using centralized tools and authentication.

Production Data Security

- Reduce the risk of compromise of Production Data.
- Implement and/or review controls designed to protect Production Data from improper alteration or destruction.
- Ensure that Confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
- Ensure Marketware, Inc. customer Production Data is segmented and only accessible to customer authorized to access data.
- All Production Data at rest is stored on encrypted volumes.
- Volume encryption keys and machines that generate volume encryption keys are protected from unauthorized access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
- Encrypted volumes use AES encryption with a minimum of 256-bit keys, or keys and ciphers of equivalent or higher cryptographic strength.

Transmission Security

- All data transmission is encrypted end to end. Encryption is not terminated at the network end point, and is carried through to the application.
- Transmission encryption keys and machines that generate keys are protected from unauthorized access. Transmission encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
- Transmission encryption keys use a minimum of 4096-bit RSA keys, or keys and ciphers of equivalent or higher cryptographic strength.
- Transmission encryption keys are limited to use for one year and then must be regenerated.
- In the case of Marketware, Inc. provided APIs, provide mechanisms to assure person sending or receiving data is authorized to send and save data.
- System logs of all transmissions of Production Data access. These logs must be available for audit.