Disaster Recovery Policy

The Marketware, Inc. Contingency Plan establishes procedures to recover Marketware, Inc. following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the Marketware, Inc. Security Officer and Privacy Officer.

The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
- *Notification/Activation phase* to detect and assess damage and to activate the plan;
- *Recovery phase* to restore temporary IT operations and recover damage done to the original system;
- *Reconstitution phase* to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out Marketware, Inc. processing requirements during prolonged interruptions to normal operations.
- Identify and define the impact of interruptions to Marketware, Inc. systems.
- Assign responsibilities to designated personnel and provide guidance for recovering Marketware, Inc. during prolonged periods of interruption to normal operations.
- Ensure coordination with other Marketware, Inc. staff who will participate in the contingency planning strategies.
- Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

This Marketware, Inc. Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a)(7), which requires the

establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

This Marketware, Inc. Contingency Plan is created under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems" dated June 2002.

The Marketware, Inc. Contingency Plan also complies with the following federal and departmental policies:

- The Computer Security Act of 1987;
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000;
- Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999;
- Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998;
- PDD 63, Critical Infrastructure Protection, May 1998;
- Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999;
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000

Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, internal malicious activities. Marketware, Inc. defined two categories of systems from a disaster recovery perspective.

- *Critical Systems*. These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if

unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.

- *Non-critical Systems*. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Applicable Standards from the HITRUST Common Security Framework

- 12.c - Developing and Implementing Continuity Plans Including Information Security

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(7)(i) - Contingency Plan

Line of Succession

The following order of succession to ensure that decision-making authority for the Marketware, Inc. Contingency Plan is uninterrupted. The Chief Product Officer (CPO) and Security Officer, Benjamin Bartel, is responsible for ensuring the safety of personnel and the execution of procedures documented within this Marketware, Inc. Contingency Plan. If the CPO and VP of Engineering are unable to function as the overall authority or chooses to delegate this responsibility to a successor, the CEO or VP of Business Development shall function as that authority. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below.

- Benjamin Bartel, CPO, CSO: 801-691-3350, ben.bartel@marketware.com
- Danny Bueno, VP of Engineering: 801783-7372, danny.bueno@marketware.com
- Tyler DeLange, VP of Business Intelligence: 407-965-6898, tyler.delange@marketware.com

Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

- The **Ops Team** is responsible for recovery of the Marketware, Inc. hosted environment, network devices, and all servers. Members of the team include personnel who are also responsible for the daily

operations and maintenance of Marketware, Inc. The team leader is the VP of Business Intelligence and directs the Ops Team.

- The **Web Services Team** is responsible for assuring all application servers, web services, and platform add-ons are working. It is also responsible for testing redeployments and assessing damage to the environment. The team leader is the VP of Engineering and directs the Web Services Team.

Testing and Maintenance

The CPO, CSO and VP of Engineering shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

Tabletop Testing

Tabletop Testing is conducted in accordance with the CMS Risk Management Handbook, Volume 2 (http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VII_4-5_Contingency_Plan_Exercise.pdf). The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

Technical Testing

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch compute and storage resources to alternate processing site.

1.Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Marketware, Inc. Based on the assessment of the Event, sometimes according to the Marketware, Inc. Incident Response Policy, the Contingency Plan may be activated by either the CPO, CSO or VP of Business Intelligence.

The notification sequence is listed below:

- The first responder is to notify the CPO. All known information must be relayed to the CPO.
- The VP of Engineering is to contact the Web Services Team and inform them of the event.
- The CPO is to begin assessment procedures with the VP of Business Intelligence.
- The CPO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CPO is to following the steps below.
- Damage Assessment Procedures:
- The CPO and VP of Business Intelligence are to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.

- Alternate Assessment Procedures:
- Upon notification from the CPO, the VP of Business Intelligence is to follow the procedures for damage assessment with combined Ops and Web Services Teams.
- The Marketware, Inc. Contingency Plan is to be activated if one or more of the following criteria are met:
- Marketware services will be unavailable for more than 48 hours.
- Hosting facility is damaged and will be unavailable for more than 24 hours.
- Other criteria, as appropriate and as defined by Marketware, Inc.
- If the plan is to be activated, the CPO is to notify and inform team members of the details of the event and if relocation is required.
- Upon notification from the CPO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The CPO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
- The CPO is to notify remaining personnel and executive leadership on the general status of the incident.
- Notification can be message, email, or phone.

2. Recovery Phase

This section provides procedures for recovering the application at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the Marketware, Inc. infrastructure at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild Marketware, Inc. infrastructure to a production state. The tasks outline below are not sequential and some can be run in parallel.

- Contact Partners and Customers affected - Web Services
- Assess damage to the environment - Web Services
- Begin replication of new environment using automated and tested scripts, currently SQL. At this point it is determined whether to recover AWS, or Azure. - Dev Ops
- Test new environment using pre-written tests - Web Services
- Test logging, security, and alerting functionality - Dev Ops
- Assure systems are appropriately patched and up to date. - Dev Ops
- Deploy environment to production - Web Services
- Update DNS to new environment. - Dev Ops

3. Reconstitution Phase

This section discusses activities necessary for restoring Marketware, Inc. operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. When the hosted data center at the original or new site has been restored, Marketware, Inc. operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

- Original or New Site Restoration
- Begin replication of new environment using automated and tested scrips, currently Salt. - Dev Ops
- Test new environment using pre-written tests. - Web Services

- Test logging, security, and alerting functionality. - Dev Ops
- Deploy environment to production - Web Services
- Assure systems are appropriately patched and up to date. - Dev Ops
- Update DNS to new environment. - Dev Ops
- Plan Deactivation

  If the Marketware, Inc. environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the Marketware, Inc. Media Disposal Policy.