Employees Policy

Marketware, Inc. is committed to ensuring all workforce members actively address security and compliance in their roles at Marketware, Inc. As such, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

Applicable Standards from the HITRUST Common Security Framework

- 02.e - Information Security Awareness, Education, and Training
- 06.e - Prevention of Misuse of Information Assets
- 07.c - Acceptable Use of Assets
- 08.j - Controls Against Malicious Code
- 01.y – Teleworking

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(5)(i) - Security Awareness and Training

Employment Policies

- All new workforce members, including contractors, are given training on security policies and procedures, including operations security, within 30 days of employment.
- Records of training are kept for all workforce members.
- Upon completion of training, workforce members complete this form.
- Ongoing security training is conducted monthly.
- Current Marketware, Inc. training can be found here: (dropbox/operations/training)
- All workforce members are granted access to formal organizational policies, which include the sanction policy for security violations.
- The Marketware, Inc. Employee Handbook clearly states the responsibilities and acceptable behavior regarding information system usage, including rules for email, Internet, mobile devices and social media usage.
- Marketware, Inc. does not allow mobile devices to connect to any of its production networks.
- All workforce members are educated about the approved set of tools to be installed on workstations.

- All new workforce members are given HIPAA training within 60 days of beginning employment. Training includes HIPAA reporting requirements, including the ability to anonymously report security incidents, and the levels of compliance and obligations for Marketware, Inc. and its Customers and Partners.
- All remote (teleworking) workforce members are trained on the risks, the controls implemented, their responsibilities, and sanctions associated with violation of policies. Additionally, remote security is maintained through the use of VPN tunnels for all access to production systems with access to ePHI data.
- All Marketware, Inc.-purchased and -owned computers are to display this message at login and when the computer is unlocked: *This computer is owned by Marketware, Inc., Inc. By logging in, unlocking, and/or using this computer you acknowledge you have seen, and follow, these policies (https://Marketware.com/policy/) and have completed this training (https://training.Marketware.com/). Please contact us if you have problems with this - privacy@Marketware.com.*
- Employees may only use Marketware, Inc.-purchased and -owned workstations for accessing production systems with access to ePHI data.
- Any workstations used to access production systems must be configured as prescribed by the Employee Workstation Use section of the Systems Access Policy.
- Any workstations used to access production systems must have virus protection software installed, configured, and enabled.
- Access to internal Marketware, Inc. systems can be requested by contacting the CSO. All requests for access much be granted to the Marketware, Inc. Security Officer.
- Request for modifications of access for any Marketware, Inc. employee can be made by contacting the CSO.