MHS

Beyond Assessments

SECURITY AWARENESS POLICY

PURPOSE

To ensure MHS employees are aware of the potential threats that exist offline as well as online, and to inform them of the responsibilities they have in securing their work premises. To minimize security breaches in MHS from a variety of threats, an annual awareness training program is conducted to inform and increase awareness of the types of threats that appear in their daily operations and how they can better protect themselves and MHS.

SCOPE

All MHS employees irrespective of the seniority, position, or their employment status will be required to complete a mandatory security training annually. Additional security training can be mandated should system changes or job roles require it. Employees are held accountable for any action that assumes their credentials.

GENERAL PRINCIPALS

1. Content

1.1. Training content will vary from year to year and will be updated to make users aware of new industry threats, with industry specified countermeasures to better protect users and assets from such threats and security best practices. Recent contents include password length, use of passphrases, phishing techniques, visual examples, ransomware, etc. Training content will vary from year to year and will be updated to make users aware of new industry threats, with industry specified countermeasures to better protect users and assets from such threats and security best practices. Recent contents include password length, use of passphrases, phishing techniques, visual examples, ransomware, etc.

2. Training

2.1. Training content will vary from year to year and will be updated to make users aware of new industry threats, with industry specified countermeasures to better protect users and assets from such threats and security best practices. Recent contents include password length, use of passphrases, phishing techniques, visual examples, ransomware, etc.

3. Time Frame and Audit

3.1. Once all users are enrolled, users will have 30 days to complete the training. Once all personnel have completed their training, users will be audited without notification of their adherence to the principles of security awareness. Training will be reviewed, updated and held annually to ensure users are kept abreast of various threat vectors.

4. Role-Based Security Awareness Training

4.1. As part of MHS risk management, MHS will provide a variety of training for specific groups with content that relates directly to specific user roles/responsibilities and requires designated users to identify the threats on such roles.

5. Clear Screen and Clean Desk

5.1. To ensure MHS information is protected from eavesdropping or other forms of access or intrusion, it is essential all employees adhere is to strict policy of ensuring their workstation log-in screens are logged off or locked when leaving their stations.

5.2. All employees must ensure their desks are clean and contain no MHS assets or documentation, irrespective if the information is sensitive or public.

Following the above procedures of this policy will ensure MHS's adherence to industry best practices, compliance to several regulations, and will ensure safety and security of our personnel and our systems. For additional questions, please contact the MHS Privacy Officer at privacyofficer@mhs.com.