Security Awareness Training and Testing Policy

Section 1. PURPOSE AND SCOPE

Technical security controls are a vital part of our information security framework but are not in themselves sufficient to secure all information assets. Effective information security also requires the awareness and proactive support of all faculty and staff, supplementing and making full use of the technical security controls. Social engineering attacks and other current exploits being used which specifically target humans rather than IT and network systems are a current example of why administrative controls are also a critical part of information security.

Without adequate information security awareness, faculty and staff are less likely to recognize or react appropriately to information security threats and incidents and are more likely to place information assets at risk of compromise. In order to protect information assets, all employees must be informed about relevant information security matters and fulfill their information security obligations.

The purpose of this policy is to specify the Clark University internal information security awareness and training program to inform and assess all faculty and staff regarding their information security obligations.

This policy applies regardless of whether staff use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of information.

Non-compliance actions will be considered an activity that jeopardizes the integrity of systems.

In general, this policy applies to all Clark University employees with access to Clark systems, networks, university information, nonpublic personal information, and/or personally identifiable information.

Section 2. PROCEDURES AND ENFORCEMENT

All awareness training must fulfill the requirements for the security awareness program as listed below:

- The information security awareness program should ensure that all faculty/staff achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.
- Additional regulatory training is appropriate for faculty/staff with specific obligations towards information security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Phishing and Social Engineering for Executives, PCI DSS, FERPA, GLBA, HIPAA and GDPR. Such training requirements must be identified in departmental/personal training plans. The training requirements will reflect your role at Clark as well as anticipated job requirements.
- Security awareness and training activities should be completed prior to access to restricted or confidential information is granted, generally through new hire security awareness training as part of the on boarding process. The awareness activities should continue on a continuous basis thereafter in order to maintain a reasonably consistent level of awareness.
- Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important, but the motivators may be different for workers focused on their own personal situations or managers with broader responsibilities to the organization and their staff.

- Clark University will provide faculty/staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

2.1 Clark University Information Security Awareness and Regulatory Training

Clark Information Technology Services (ITS) in conjunction with the Human Resources office require that each employee upon hire complete a new hire security awareness training module which is approximately one hour of online training. As of January 2023, the module contains: 'New Hire's Guide to Security Awareness' (10 min) Module, 'FERPA (Education)' (9 min), 'PII and You (20 mins), 'Social Engineering Foundations' (10 min), 'Using the Phish Alert Button - Report Suspicious Emails Using Microsoft Outlook' (7 min) and at least annually thereafter successfully complete 'Security Awareness Foundations' (25 min) Module, and annually review and accept the "Confidentiality and Privacy Agreement". Modules are subject to change as some modules may be retired or replaced by newer content at the discretion of ITS & HR. New hires are also required upon completing the previously mentioned trainings to review and accept the "Appropriate Use Policy", "Data Classification Policy", "Data Security Policy for All Faculty, Staff and Student Employees", and "Confidentiality and Privacy Agreement". Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. New hires will be given 30 days to complete onboarding Security Awareness Training.

2.2 Simulated Social Engineering Exercises

Clark University ITS will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. These tests will be conducted periodically throughout the year with no set schedule or frequency. Targeted exercises against specific departments or individuals may be warranted based on a risk determination. Risk factors can include types of data an employee hands, types of security access, involvement in particular industries known to be a high risk for Cybercrime.

2.3 Remedial Training Exercises

From time-to-time Clark University employees may be required to complete additional training courses or may be required to participate in additional training exercises as part of a risk-based assessment.

Section 3. COMPLIANCE & NON-COMPLIANCE WITH POLICY

Compliance with this policy is mandatory for all employees. Clark University ITS in conjunction with Human Resources will monitor compliance with this policy and report to supervisors any instances of non-compliance with this policy.

Certain actions or non-actions by Clark University personnel increase risk of an information security incident and will be considered a non-compliant action. A sample of these actions are:

- Submitting information as part of a real or simulated attack
- Taking detrimental action to a real or simulated attack (e.g. opening attachment, clicking link, running code, replying, etc…)
- Failure to complete required training within the time allotted
- Failing to follow company policies in the course of a social engineering exercise

Section 4. RESPONSIBILITIES AND ACCOUNTABILITIES

Listed below is an overview of the responsibilities and accountabilities for managing and complying with this policy program.

The Information Privacy and Compliance Analyst is accountable for running an effective information security awareness and regulatory training program that informs and motivates workers to help protect the organization and the organization's customer's information assets while safeguarding through regulatory requirements as part of their employment with Clark University.

The Information Privacy and Compliance Analyst is responsible for developing and maintaining a comprehensive suite of information security policies, standards, procedures and guidelines that are to be mandated and/or endorsed by senior leadership where applicable. Working in conjunction with other corporate functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of employee responsibilities identified in applicable policies, laws, regulations, contracts, etc.

All Managers or Department Chairs are responsible for ensuring that their staff and other workers within their responsibility participate in the information security awareness, training, and educational activities where appropriate and required.

All Faculty and Staff are personally accountable for completing the security awareness and regulatory training activities, and complying with applicable policies, laws, and regulations at all times.

Related Policies and Regulations

- HR/ Employee Handbook (PDF)
- Written Information Security Policy (WISP)
- Acceptable Use Policy

History/Revision Information

Responsible Office/ Division: The Vice President for Information Technology & CIO is charged with the responsibility to periodically review the policy and propose changes as needed. When required, they will consult with the Office of Human Resources. Failure to adhere to the provisions of this policy statement may result in loss of Clark University access privileges; and could lead to disciplinary action taken by Human Resources.

This policy will be updated and re-issued at least annually to reflect, among other things, changes to applicable law, update or changes to Clark University requirements, technology, and the results or findings of any audit.

Effective Date: March 25, 2024
Last Amended Date:
Next Review Date: March 25, 2025