Regis ITS Secure HIPAA Network Testing Policy

Policy Statement/Purpose

The Regis ITS Secure HIPAA Network Testing Policy defines the methodology that minimizes the exposure to potential exploits that are a threat to the Regis Secure HIPAA network. These guidelines are designed to protect and secure the confidentiality, integrity, and availability of the University's electronic information and data that are subject to the HIPAA Privacy and Security Rules.

Scope

This policy applies to all Regis systems and devices in the secure HIPAA networks that transmit manipulate or store the University's electronic information and data covered by HIPAA requirements.

Policy Compliance and Sanctions

Systems, resources, administrator activities and processes will be monitored to verify proper operation of the department's information security practices. All violations of the ITS HIPAA Secure Network Testing Policy should be reported to the ITS Information Security Officer.

In addition, if the violation impacts any of the University's HIPAA security policies or associated practices, it shall also be reported to the Regis HIPAA Privacy & Security Committee.

Serious or repeat violations will, when appropriate, be reported to the Human Resources Department or Legal Counsel for follow-up.

Definitions and Terms

The term "User" includes any individual that has been granted general user access to any of the University's general technology resources or information assets. Regis Users include students, faculty, staff, permanent and temporary employees, vendors, third-party service providers, and subcontractors.

The term "Event" applies to a data record generated by specific system, application or user activities. Events are typically generated on an individual basis, though multiple events may be generated by a series of tasks required to complete an activity.

The term "Log File" applies to any designated area where generated events are collected and stored.

The term "Technology resource" applies to any technology-related asset owned, leased, or controlled by the university including:

- Software assets (e.g.: application software, system software, development tools, utilities);
- Hardware assets (e.g.: workstations, laptops, mobile devices, removable storage devices, mainframe, peripherals, network equipment, system devices);
- Communications services (e.g.: e-mail, Internet, phone, voice mail); and
- Other electronic technologies deployed within the University's networked environment.

Vulnerability management program

The Vulnerability Management Program consists of vulnerability scanning, penetration testing and remediating vulnerabilities.

- The types and frequency of the tests to be performed by the Regis ITS Department must be established and performed in accordance with a defined schedule that supports timely discovery of security vulnerabilities.
- Additional testing beyond the designated frequencies may be required based on significant changes to the networks, rescanning to validate remediation efforts were successful, or when determined necessary by the ITS Department managers.

Vulnerability scanning

A vulnerability scan provides an overview of the flaws that exist on the system by enumerating network, host and application vulnerabilities.

- Discovered vulnerabilities represent potential threats to network, systems and data resources.
- Vulnerability analysis is focused on identifying, quantifying and rating the security vulnerabilities in a system.
- Vulnerability analysis is focused on identifying, quantifying and rating the security vulnerabilities in a system.
- Vulnerability scans should be performed by personnel with the knowledge and experience in network and application vulnerability scanning using scanning tool that can readily detect and assess common vulnerabilities.

Wireless scanning

The purpose wireless scanning is to look for any unauthorized or rogue wireless device introduced into an organization's network or allows unmanaged and unsecured WLAN access.

- Wireless is currently not used within the Regis Secure HIPAA network.

Penetration testing

Penetration testing provides an analysis of the possible impact of flaws and vulnerabilities on the underlying network, operating system, databases etc. Penetration testing attempts to exploit the flaws and vulnerabilities to determine whether unauthorized access or other malicious activity is possible and to identify the potential harm that could result from the unauthorized access.

- Penetration testing should include network and application layer testing and should occur from both outside the network trying to come in (untrusted sources) and from inside the network (trusted sources).
- Testing must be conducted by experienced testers who are organizationally separate from those personnel who manage the security devices and systems being tested.
- An experienced tester would have two to three years of information security assessment experience in designing and conducting common penetration testing activities that assess the most the likely intrusion points into an organization's network through conducting information gathering and network enumeration activities, launching exploits with a chosen exploit framework, conducting privilege escalation activities and post-exploitation information gathering.

Remediation

Remediation is the process of methodically addressing discovered security flaws and deficiencies that pose a threat to the infrastructure it they were to be exploited. A comprehensive approach to remediation may include any or all activities such as configuration changes, architecture changes, patching or updating software at a device, system or application level.

- Where possible, High Risk vulnerabilities should be remediated within 30 days of discovery.
- The order for remediating vulnerabilities should take into consideration the device's location of the device, system or application with the discovered vulnerabilities within the infrastructure and its use or access to sensitive information assets.
- Compensating controls should be considered for vulnerabilities that cannot be remediated using a patch or an update.