REGIS UNIVERSITY

Regis ITS Secure HIPAA Network Physical Security Policy

Policy Statement/Purpose

The Regis ITS Secure HIPAA Network Physical Security Policy defines the guidelines to be used by the Regis ITS Department to control and limit physical access to the facility, devices, systems and databases located within the University's 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. This policy also applies to all ITS Department administrators who manage and/or access to networks, systems, devices, programs, equipment, or applications in the secure HIPAA networks.

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 Physical Security 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 "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.

General physical security requirements

The minimum physical security required to ensure the integrity and safety of the University's secure HIPAA networks and information assets, employees, and visitors is maintained by:

- Keeping office entry points clear of obstacles that restrict visibility of the surrounding area,
- Securing exterior office doors with mechanical or electronic locks, and
- Segregating areas inside the office space, where necessary, through the use of security zones.

ITS facility physical security zones that host the secure HIPAA networks

Physical security zones are segregated areas within the facility or location that have differing physical security requirements. There are three types of physical security zones:

- Public Areas
- Controlled Areas
- Secure Areas

The security requirements of each zone are determined by a risk assessment that is based on:

- The protection and safety of the people and the business operations being performed within the zone,
- The sensitivity of the information assets contained or that are accessible from within the zone, and The technology resources located in the zone

The ITS Department will maintain a floor plan of the ITS facility areas and locations that clearly identifies the physical security zone assignment of the physical area.

- The appropriate physical security controls must be implemented and maintained for each identified zone.
- Physical access by all personnel entering the controlled and secure areas must be controlled by rights based on the individual's assigned roles and responsibilities. Access will be limited to only those areas necessary to perform their duties

Public areas: Regis Secure HIPAA Networks

Public areas are physical areas designated for conducting routine business and operations with the University's users, partners and preferred vendors. Requirements of a public area include:

- Access points into the office are not restricted.
- Everyone has free ingress and egress to the area.
- No escorts are required.

There are no public areas for the facility areas that host the University's Secure HIPAA Networks.

Controlled areas: Regis Secure HIPAA Networks

- Controlled areas are physical areas that have additional physical security controls beyond the public area requirements that are adjacent to and allow access to the University's Secure HIPAA Networks. Requirements of a controlled area include:
- A defined security perimeter that includes security barriers such as physical entry controls that effectively restrict physical access to only authorized personnel on a 24 X 7 basis.
- Physical access must limit access to only those individuals necessary to perform their assigned duties.
- All visitors in a controlled area must follow the log in procedures.

Secure areas: Regis Secure HIPAA Networks

- Secure areas are physical areas that have additional physical security controls beyond the secure area requirements to specifically protect those areas of the facility that host the devices and systems that comprise the University's Secure HIPAA Networks. Requirements of a secure area include:
- A defined security perimeter that includes security barriers and physical entry controls that

effectively restrict physical access to only authorized personnel on a 24 X 7 basis.

- Physical access must limit access to only those individuals necessary to perform their assigned duties.
- All visitors in a secure area must follow the log in procedures and must have an escort while in the secure area.
- No photographic, video, audio or other recording equipment, mobile computing devices and portable media collection devices may utilized in the secure areas without prior authorization.

Facility controls for secure areas hosting the secure HIPAA networks

The hosting facility shall document all installations, repairs and maintenance that affect security of the hosting facility, such as hardware, walls, doors, and locks.

- All repairs and modifications to the physical components of the hosting facility which are related to security (for example, hardware, walls, doors, and locks) must be documented.

Emergency access

Each location's physical security procedures must contain provisions for providing physical access as required by emergency personnel, such as police or the fire department, who are responding to or investigating events at the location pertaining to the safety and protection of lives, property and university assets.

Physical access monitoring and notifications of unauthorized physical access

- Where possible, physical access to the University’s secure areas assigned to the secure HIPAA network location should be monitored on a 24 X 7 basis.
- The appropriate personnel must be notified in the event of an alarm or detection of suspicious activity.
- The University’s ITS department personnel should follow the University’s standard physical security reporting processes if they encounter unauthorized personnel in any of the secure areas.
- In addition the appropriate ITS Department Managers and the ITS Information Security Officer should be notified if the unauthorized physical access includes any areas that host the University’s Secure HIPAA Networks.