Regis ITS Secure HIPAA Network Logical Access Policy

Policy Statement/Purpose

The Regis ITS Secure HIPAA Network Logical Access Policy defines the guidelines to be used by the Regis ITS Department to control logical access to the 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 Logical Access 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 "Administrator" applies to any individual that has been granted elevated privileges that allow access beyond the general user access levels for the purposes of installing, monitoring, maintaining and troubleshooting the University's technology resources or information assets. Administrator access includes access levels and privileges associated with roles commonly referred to as administrative, root and superuser accounts.

The term "Logical Access Control" is defined as the ability to permit or deny the use of electronic information assets and technology resources based on logins which establish identification, authentication, and authorization

The term "Privileged Access" is used to denote a level of access that allows the individual to bypass, override or modify a system or security control.

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 assignment and approval of access rights

- Logical access rights within the secure HIPAA network are granted to users based on the need to know and/or access electronic data and information. A formal record is maintained on all authorized users and their assigned user access rights. There are two types of logical access rights: standard access and privileged access.

Standard Access

- Standard access provides only the necessary logical access to system resources for authorized individuals who are performing routine functions within a defined University role.
- Individuals approved for standard access will be assigned a unique user access ID for authenticating their access and to ensure individual user activities can be monitored.
- Standard access rights are assigned to new users based on the standard access levels associated with the logical access required to carry out the standard tasks of the person's role in the organization.
- Modifications to assigned user access rights must be requested using the University's standard process for handling technology users' requests and approved by the appropriate university managers. This includes changes necessary to reflect access changes based on position transfers and/or the addition or removal of job responsibilities.
- Termination of access shall be implemented upon the timely receipt of the University's standard reporting processed by Human Resources reports.
- As necessary during a potential security incident, the ITS Information Security Officer may remove use logical access to support standard incident response procedures.

Privileged access

Privileged access rights are typically assigned to network administrators or system administrators and are additional access levels that go beyond the standard user access. The criterion for standard access as defined above also applies to privileged access.

- Privileged access rights shall be granted only to individuals whose assigned duties and responsibilities require that level of access. The privileged access shall not compromise the segregation of duties.
- All privileged access requests for the secure HIPAA networks must be approved by the ITS Information Security Officer and the department manager who has ownership of the electronic information asset or technology resource for which privileged access is being requested.
- Privileged access shall be approved based on a permanent need-to-use basis or for an event-by-event basis. Access granted for an event-by-event basis shall be removed once the access is no longer needed.
- Where an individual is both a university user (such as a student) and a university employee who requires network or system level administrative access to the devices or systems within the secure HIPAA networks, the individual should have separate user and privileged access accounts.

Event logging of logical access

User access and privileged user access shall be logged in accordance with the ITS departments Log & Event Management Policy.

Reviews of logical access rights

- Assigned logical access rights shall be reviewed on a regular basis to ensure that they are limited to those with a business need.
- Logical access for terminated employees shall be immediately deactivated.
- Annually, the ITS Information Security Officer shall review user access and privileged user access to ensure the assigned access accurately reflects the logical access level required for each user who has access to electronic data and information or to the devices and systems that comprise the University’s secure HIPAA network.