Regis User Password Policy

Policy Statement/Purpose

The Regis User Password Policy establishes the general password guidelines and overall strategy for creating, using, changing, monitoring and safeguarding passwords used to validate a Regis user's identity for access to Regis information systems and data. These guidelines are designed to protect and secure the confidentiality, integrity, and availability of the university's electronic information and data.

Scope

This policy applies to all Regis Users with general user access to the university's technology resources such as access to networks, systems, devices, programs, equipment, or applications that transmit, manipulate or store the university's electronic information and data.

Policy Compliance and Sanctions

Systems, resources, user activities and processes will be monitored to verify proper operation of the university's information security practices. All violations of the university's User Password Policy should be reported per the University's information security reporting processes.

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 user password management

- All Regis users that require access to Regis networks, systems, devices, programs, equipment, or applications must apply for a unique user identification.
- All Regis users must supply a password in conjunction with their unique user identification to gain access to any Regis network, system, device, program, equipment or application used to access, create, transmit, receive, or store electronic information and data.
- The password aging schedule and password structure rules will be based upon the risk-level of the network system, application, program, device, and equipment.
- Wherever possible, Regis's network systems, applications, programs, devices, and equipment must be configured to automatically disable a user's password after the threshold for unsuccessful login attempts is exceeded. Deactivation will last for a 60 minutes.
- Terminations and changes in status or position will be communicated to the ITS department to enable modification or revocation of a user's password in a timely manner.
- Adherence to the password practices will be monitored and periodic random testing of passwords may be performed by the Information Security Officer. If a password is guessed or cracked during one of these tests, the Regis user will be required to change it and sanctions may apply.

User password construction guidelines

The use of a "strong password" is required on all systems. A strong password consists of the following:

- A minimum of eight (8) characters in length
- Contains at least 3 of the following:
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Punctuation characters
    - Special characters
- Is not based on any dictionary word, in any language.
- Is not derived from easily-guessed or public information about the user such as family member names, birthdays, pet names, addresses, phone numbers, etc.
- Is not a previously used password followed by a digit.

User password protection practices

Regis Users will comply with the following rules regarding use of passwords:

- All user passwords must be changed according to the schedule set forth by the university's administration.
- The re-use of passwords will not be allowed for twelve (12) calendar months.
- Users should not use the same password for gaining access to publicly available websites as they do for gaining access to Regis's systems or applications.
- Passwords for access to Regis systems or applications must not be displayed in public view. "Public places" include, but it not limited to , monitors, keyboards, bulletin boards, walls, or back of ID badges.
- Regis user passwords must not be inserted as plain text into email messages or other forms of electronic communication.
- Regis user passwords must not be revealed to anyone including family members, co-workers, and

supervisors.

- Written passwords must be stored in a secure location; electronic passwords must not be stored on any computer system or device, including mobile devices, without encryption of the password.
- If a Regis User feels that his or her account or password has been compromised, they must report the incident immediately to the Information Technology Services Help Desk which will initiate an immediate change of the affected user's passwords.

Comment [LP1]: Read the comments by SC & CS; this one could be considered redundant to the bullet immediately following so I removed it.