Regis ITS Department Password Policy

Policy Statement/Purpose

The Regis ITS Department Password Policy establishes the password guidelines and strategy for creating, using, changing, monitoring and safeguarding "Administrator", "System" and "Service" account passwords used 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 ITS Department administrators and system or service accounts with system-level privileges used to access 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, administrator activities and processes will be monitored to verify proper operation of the department's information security practices. All violations of the ITS Department Password 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 terms "System Level Account" and "Service Account" apply to accounts that are used to access the University's technology resources and information assets and do not correspond to an actual person. These accounts are often built-in accounts that the systems and services use to access resources they need to perform their activities.

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 "Administrator" password management

- All Regis ITS department personnel that require system-level access to Regis networks, systems, devices, programs, equipment, or applications must apply for an Administrator password account that has a unique user identification.
- In the event an Administrator has both an administrator and a general user account, the administrator user identification must not be the same as the individual's general user account.
- All Regis administrator accounts 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 for administrator passwords will be set by the Information Security Officer 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 ISO 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.

"System" and "Service" accounts password management

- All Regis System or Service Accounts that require system-level access to Regis networks, systems, devices, programs, equipment, or applications must be assigned a unique identifier.
- All System or Service Accounts must supply a password in conjunction with their unique identifier 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.
- System and Service Accounts passwords, wherever possible, should be unique.
- The password aging schedule and password structure rules for System and Service account passwords will be set by the Information Security Officer based upon the risk-level of the network system, application, program, device, and equipment.

User password construction guidelines

The use of a "strong password" is required on all systems, where supported. 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 on the user such as family member names, birthdays, pet names, addresses, phone numbers, etc.
- Is not a previously used password followed by a digit.

- In addition any system or service account password that provides access to the administrative functions of the systems or devices must not be a vendor-supplied or default password.

Administrator, "System" and "Service" account password protection practices

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

- All Administrator, "System" and "Service" account passwords must be changed according to the schedule set forth by the ITS Information Security Officer.
- The re-use of passwords will not be allowed for twelve (12) calendar months.
- All "Administrator", "System" and "Service" account passwords will be rendered unreadable during transmission and storage using strong cryptography.
- Regis administrator's passwords must not be revealed to anyone including family members, co-workers, and supervisors.
- Regis system and service account passwords may be shared based on "need to know" for the performance of authorized tasks.
- If a Regis administrator feels that his or her account or password has been compromised, or system or service 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.