Establishing and Maintaining an Information Security Program

Introduction

Regent University continually develops, maintains and improves its Information Technology (IT) infrastructure and applications to support the creation, storage, modification and sharing of data. Our IT systems are essential to the operation of the University. The University, therefore, has a responsibility to institute appropriate safeguards to keep its IT systems and information assets secure. In addition, the University must comply with various regulatory requirements that are also designed to keep certain types of data secure and confidential.

The security of IT systems and information assets is dependent on the individuals managing as well as the individuals utilizing such resources. The University is committed to supporting the principles of academic freedom and the free exchange of ideas and the University's information security policies and programs are intended to support those principles while still maintaining an appropriate level of security.

The goals of this security program are to:

1. Creating controls and defining good technical practices to support a dependable Information Technology Network.
2. Protect the University's IT systems and information assets from unauthorized access, alteration, disclosure or destruction.
3. Ensure the reliability and availability of the University's IT systems and information assets.
4. Ensure the privacy of faculty, staff and student information and that of other University customers or associates.
5. Identify and prevent identity theft.
6. Protect the reputation of the University and ensure compliance with federal and state laws and regulations.
7. Establish resources and guidelines that allow all individuals within the University community to practice good data stewardship.

General Privacy Policy

Regent University carefully protects all nonpublic personal information in our possession regarding students and their families. The School will not release nonpublic, private, personal, or financial information about our students or applicants to any third party, except as specifically provided in this policy. The School will release certain nonpublic personal information to federal and state agencies, government contractors, student loan providers/servicers, and other parties as necessary for the administration of the federal student aid programs, for enforcement purposes, for litigation, and for use in connection with audits or other investigations. Disclosure is permitted to law enforcement or emergency services agencies in the performance of their duties or when student safety or health may be in jeopardy. The School will not sell or otherwise make available personal information for marketing purposes to any third party at any time.

Recourse for Noncompliance

In cases where Regent University resources are actively threatened, the Regent Information Technology Department will act in the best interest of the University by securing the resources.

The Regent Information Technology Department will abide by the incident handling procedures to mitigate the threat. In an urgent situation requiring immediate action and leaving no time for collaboration, the Regent Information Technology Department is authorized to disconnect any affected device from the network. University resources are subject to "vulnerability assessment" and safeguard verification by the Regent Information Technology Department.

Individuals who are subject to but do not comply with this policy and mandatory implementation of standards will be subject to remedial action in accordance with University policies and procedures

(including but not limited to the Student Code of Conduct, Code of Intellectual Property Rights, Classified Staff Human Resources Policy Manual, and the policy on the Acceptable Use of Computers/Networks and Non-Disclosure Agreement) or contract terms, as appropriate. Violations of this policy may result in loss of data access privileges, administrative sanctions, and personal civil and criminal liability.

Exceptions

The Regent Information Technology Department may grant exceptions to this policy and/or standards after preliminary review.

System Access Control

Regent University has an obligation to effectively protect the intellectual property and personal and financial information entrusted to it by students, employees, partners and others. Using passwords that are difficult to guess is key step toward effectively fulfilling that obligation.

Regent University strictly enforces a password policy:

- Multi-factor complexity
- Expiring every 6 months
- Passwords stored electronically are not stored in readable form where unauthorized persons might discover them.

- Passwords may not be written down and left in a place where unauthorized persons might discover them.
- Passwords may never be shared or revealed to anyone other than the authorized user.

If a password is suspected of being disclosed or known to have been disclosed to anyone other than the authorized user, it is required to be changed immediately.

Password System Set-Up

All computers permanently or intermittently connected to Regent University local area networks must have password access controls. If the computers contain confidential or protected information, an extended user authentication system approved by the Information Technology department must be used. Multi-user systems (servers) should employ user IDs and passwords unique to each user, and user privilege restriction mechanisms with privileges based on an individual’s need to know. Network - connected, single - user systems must employ hardware or software controls approved by Information Technology that prevent unauthorized access.

All vendor - supplied default fixed passwords must be changed before any computer or communications system is used in production. This policy applies to passwords associated with end-user user IDs and passwords associated with privileged user IDs.

Where systems software permits, the number of consecutive attempts to enter an incorrect password is strictly enforced. After five unsuccessful attempts to enter a password, the involved user ID must be suspended until reset by a system administrator or temporarily disabled for no less than three minutes. The VPN and Web Enabled Mail constant connections must have timeout periods and logged out upon reaching the threshold.

Whenever system security has been compromised or if there is a reason to believe that it has been compromised, the involved system administrator must immediately take measures to ensure that passwords are properly protected. This includes but not limited to; resetting user account credentials, isolating any currently/previously hardware in contact with the compromise.

Logon and Logoff Process

All users must be positively identified prior to being able to use any Regent University multi-user computer or communications system resources. Positive identification for internal Regent University networks involves a user ID and password, both of which are unique to an individual user.

Positive identification for all Internet and remote lines involves the use of automated authentication techniques. Multi-factor authentication is enforced at Regent University to access to our internal systems and/or networks. Modems, wireless access points, routers, switches or other devices attached to network-connected workstations located in Regent University offices are forbidden unless they meet all technical requirements and have been approved by the Information Technology department.

Data and Program Backup

Personal computer users are responsible for backing up the information stored on their local machines. For multi-user computer (servers) and communication systems, a system administrator is responsible for making periodic backups.

To ensure that valuable or critical data is backed up, it must be stored on network servers managed by the Information Technology department or a trusted partner.

Regent University requires the use of industry-standard media, techniques, and timelines in executing all backups. For multi-user computer systems, whenever systems software permits, backups must be performed without end-user involvement, over an internal network and during the off hours.

Designated Coordinators

Jonathan Harrell – Assistant Vice President of Information Technology

Steve Baskerville – Director of Network Engineering

Ben Golub – Security Engineer

Threat Monitoring

Active monitoring of the internal Regent network is accomplished both internally using various security controls and appliances such as intrusion detection and prevention systems, active scans and virus protection and reporting software which is installed on all Regent assets. Active monitoring of all inbound and outbound traffic is also conducted by REN-ISAC a Computer Systems Incident Response Team (CSIRT) for higher education in the U.S.

Network Isolation and Segmentation

To increase network security Regent University implements both physical and virtual LAN segmentations. Each of these segments have IP subnet boundaries establishing isolation of critical and sensitive data, out of reach of any Public, Guest or Student networks. Regent University has automated authentication protocols in place to ensure proper VLAN assignments of devices joining our internal networks.

Risk Assessment

Risk assessments/Audits are conducted Semi-annually both internally and by a certified third party vendor. Once a risk has been identified steps are taken to determine the extent of the threat, evaluation, decision and action to remediate the threat. Finally documentation and After Action Review of the threat remediation is conducted by our Emergency Preparedness Committee.