University of Portland

NETWORK SECURITY POLICY

1. **PURPOSE:** The purpose of this policy is to define criteria and protocols for assessing risk, preventing data loss and responding to incidents.

2. **SCOPE:** Without a security policy, the availability of the University's network can be compromised. This policy begins with assessing the risk to the network and building a team to respond. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. Lastly, the review process modifies the existing policy as needed and adapts to lessons learned.

3. **POLICY:** This policy outlines three phases of network security: preparation, prevention, and response.

   a. **Preparation:** Users' roles and responsibilities regarding security are outlined in the Acceptable Use Policy and Information Security Policy. Additionally, the Vice President for University Operations maintains a confidentiality agreement that is used in the consideration of possible vendor transactions or relationships.

   - **Administrator Acceptable Use Statement:** The Director for Technical Services is hereby responsible for developing and maintaining an administrator acceptable use statement to explain the procedures for user account administration, policy enforcement, and privilege review. The Director of Technical Services will ensure that administrator requirements listed in the acceptable use policy are reflected in training plans and performance evaluations. Specific policies concerning user passwords and the handling of data are contained in the Password Policy and Information Security Policy respectively.

   - **Risk Analysis:** As part of the preparation phase, the Director of Technical Services; in coordination with the Chief Information Officer, Director of Academic Technology Services, and Director of Web and Enterprise Services will conduct a risk analysis to identify the risks to the network, network resources, and data. The intent of the risk analysis is to identify portions of the network, assign a threat rating to each portion, and apply an appropriate level of security. This helps maintain a workable balance between security and required network access. Each network resource will be assigned one of three risk levels:

     - ***Level 3 - Low Risk*** – Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the institution or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.

     - ***Level 2 – Medium Risk*** – Systems or data that if compromised would cause a moderate disruption to the institution, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.

     - ***Level 1 - High Risk*** – Systems or data that if compromised would cause an extreme disruption to the institution, cause major legal or financial ramifications, or threaten the health or safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the institution or other systems.

     The Director of Technical Services will assign a risk level to each of the following: core network devices, distribution network devices, access network devices, network monitoring devices, network security

devices, email systems, network file servers, network print servers, network application servers (e.g., DNS and DHCP), data application servers (e.g., Oracle, SQL), desktop computers, and other devices (networked and standalone). Once a risk level is assigned, it is necessary to identify the types of users of that system as follows:

- *Administrators* – Internal users responsible for network resources.
- *Privileged* – Internal users with a need for greater access.
- *Users* – Internal users with general access.
- *Partners* – External users (also called Vendors) with a need to access some resources.
- *Others* – External users who are not considered partners/vendors.

The identification of the risk level and the type of access required of each network system forms the basis of a security matrix. The security matrix provides a quick reference for each system and a starting point for further security measures, such as creating an appropriate strategy for restricting access to network resources.

- **Security Team:** The Chief Information Officer will lead a security team comprised of IS Directors, the Infrastructure Manager, the Tech Support Manager, and the Information Security Analyst(s). The security team has three areas of responsibility: policy development, practice, and response. Policy development is focused on establishing and reviewing security policies for the institution on an annual basis, to include the risk analysis. Practice is the stage during which the security team conducts the risk analysis; the approval of security change requests; reviews security bulletins and alerts from vendors, REN-ISAC, and other mailing lists; and turns plain language security policy requirements into specific technical implementations. The last area of responsibility is response. While network monitoring often identifies a security violation, it is the security team members who manage the actual troubleshooting and fixing of such a violation. Each security team member should know in detail the security features provided by the equipment in his or her operational area and be able to assign resources to implement resolutions.

b. **Prevention:** Prevention is broken down into two parts: approving security changes and monitoring security of the network.

- **Approving Security Changes:** Security changes are defined as changes to network equipment that have a possible impact on the overall security of the network. The Infrastructure Manager and the Information Security Analyst are responsible for proposing security changes to Change Advisory Board (CAB) for approval. Examples include, but are not limited to, the following:

  - Any change to the firewall configuration.
  - Any change to the access control lists (ACL).
  - Any change to Network Access Control configurations.
  - Any change or update in software that differs from the approved software revision level list as reflected in the master software library.

  Any member of the CAB can deny a change request that is considered a security change until it has been approved by the security team. In emergency situations, the Infrastructure Manager and the Information Security Analyst can authorize security changes providing such changes are immediately brought to the attention of the security team.

- **Monitoring the Network:** Security monitoring is similar to network monitoring, except it focuses on detecting changes in the network that indicate a security violation. The starting point for security monitoring is determining what is a violation. In conducting a *Risk Analysis*, the security team identifies the level of monitoring required based on the threat to the system. In *Approving Security Changes*, the

security team identifies specific threats to the network. By looking at both parameters, the security team will be able to develop a clear picture of what needs to be monitored and how often. Low-risk equipment will be monitored weekly, medium-risk equipment daily, and high-risk equipment hourly.

c. **Response:** Response is broken into three parts: security violations, restoration, and review.

- **Security Violations:** When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having guidelines in place to make these decisions ahead of time makes responding to an intrusion much more manageable. The security team is responsible for developing a notification system that is available 24 hours a day, 7 days a week. Additionally, the security team is responsible for defining the level of authority given to the Infrastructure Manager and the Information Security Analyst to make changes and in what order the changes should be made. Possible corrective actions are:

  - Implementing changes to prevent further access to the violation.
  - Isolating the violated systems.
  - Contacting the carrier or ISP in an attempt to trace the attack.
  - Using recording devices to gather evidence.
  - Disconnecting the violated systems or the source of the violation.
  - Contacting the police, or other governmental agencies.
  - Shutting down violated systems.
  - Restoring systems according to a prioritized list.
  - Notifying internal managerial and legal personnel.

  To determine the extent of the violations, the security team will do the following:

  - Record events by obtaining sniffer traces of the network, copies of log files, active user accounts, and network connections.
  - Limit further compromises by disabling accounts, disconnecting network equipment from the network, and disconnecting from the Internet.
  - Backup compromised systems to aid in a detailed analysis of the damage and method of attack.
  - Look for signs of compromise. Often when a system is compromised, there are other systems or accounts involved.
  - Maintain and review security device log files and networking monitoring log files, as they often provide clues to methods of attack.

- **Restoration:** Restoration of normal network operations is the final goal of any security violation response and is defined in the Technology Availability Plan (TAP).

- **Review:** The review process is the final effort in creating and maintaining a security policy. The Network Security Policy should be a living document that adapts to an ever-changing environment. As such, the security team will review the existing policy on a continual basis against known best practices, lessons learned, REN-ISAC security practices, security improvements, bulletins, alerts, etc. The Vice President for University Operations will employ the services of an outside firm that specializes in security to penetrate the network and test not only the posture of the network, but the security response of the organization as well. Such tests will be conducted on an annual basis. This review is intended to identify gaps in procedures and training of personnel so that corrective action can be taken.

4. **EXCEPTIONS:** Exceptions must be approved, in writing, by the Vice President for University Operations.

5. **SANCTIONS:** Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University Fpolicy. Any violation of thi
s
policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.