California University of Pennsylvania
Pennsylvania System of Higher Education

Technology Policy Number 2010-03
Extranet Connection Policy

Approved by:

History: Issued – 11/10/10

Revised --

Additional History

Related Policies:

Additional References:

I. Introduction

An extranet is a computer network that allows controlled access from the outside, for specific business or educational purposes. An extranet can be viewed as an extension of a Universities intranet that is extended to users outside the University, usually partners, vendors, suppliers, or other Third Party organizations.

II. Purpose

This policy outlines the procedures that Third Party organizations must follow when connecting systems to the California University of Pennsylvania Network. The purpose of the policy is to protect the confidentiality, integrity, and availability of University data, and to protect California University of Pennsylvania's computing and network infrastructure.

III. Statement of Policy

1. **Security Review – All new extranet connectivity requests will go through a security review by the Security, Quality, and Compliance Team. The reviews are used to ensure that all access matches the business requirements in the best possible way. To ensure that patches and security**

on systems are adequate, periodic vulnerability scans may be performed without notice.

2. **Business Case – All production Extranet connections must be accompanied by a valid business justification, in writing, that is approved by the University.**
3. **Point of Contact – The 3rd Party must designate a Point of Contact (POC) for the Extranet connection.**
4. **Establishing Connectivity – Prior to gaining Extranet connectivity, the 3rd Party must provide documents that detail the protocols, ports, and services that their system(s) will use for connectivity.**
5. **Changes in Access – All changes in access must be accompanied by a valid business justification and are subject to a Security Review. Changes are implemented via a corporate Change Management Process.**
6. **AUP – All connectivity and use must conform to California University of Pennsylvania Acceptable Use Policy.**
7. **Basic Requirements for Connecting Devices**
    a. **Passwords**
        i. **Devices must be protected by strong passwords that are resistant to dictionary attacks.**
        ii. **Default passwords and blank passwords must never be used.**
        iii. **Passwords must be encrypted in transit and in storage.**
        iv. **Guest or anonymous access should be disabled.**

    b. Security Patches – Security patches shall be applied on a timely basis.

    c. Antivirus Software – Devices running Windows and Macintosh Operating Systems must run antivirus software with up-to-date definitions.

    D. Unneeded Services- Disable or uninstall any unneeded services. If you do not use services such as ftp, telnet, snmp, http, etc. then they should be disabled.

    E. Use Secure Protocols- Use protocols such as ssh instead of telnet, sftp instead of ftp, https instead of http, and SNMPv3 instead of SNMP. Telnet, ftp, http, and SNMP are clear-text protocols.

    F. Sensitive Information- No sensitive information is to be stored on these systems.

G. Backup and Recovery- Backups should be performed regularly by the Third Party.

IV. Definitions

1. **Third Party – A business that is not a formal or subsidiary part of California University of Pennsylvania.**