Information Technology Policy

9.3000

IT Security for IT and Data Professionals

Security Controls

This section outlines the basic and derived security requirements as outlined in NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

A firewall is required at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.

Only port 80 and port 443 (unencrypted and encrypted web traffic) are allowed through the firewall by default. All other outbound connections must be granted via specific firewall rules, and limited to known IP addresses or IP address ranges.

NOTE: This control also addresses in part PCI DSS Requirement #1, Install and Maintain a Firewall Configurati
to Protect Cardholder Data

3.1.21 Limit use of organizational portable storage devices on external information systems.

This will be addressed in 9.2000, End User Responsibilities, and addressed in End User training (see section 3.2, Awareness and Training).

3.1.22 Control information posted or processed on publicly accessible information systems.

MU Internal and Confidential data shall not be posted or processed on public information systems. The Director, Marketing and the CIO have responsibility for monitoring compliance with this policy.

AU uses the NTP (Network Time Protocol) to maintain accurate time on all servers, workstations and network lw5tet-

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Two-factor authentication is required for VPN access to the AU network, and for login to all administrative may be set to never expire, but must also be defined to prevent direct login. The definition of service accounts would include any database accounts used by applications to access the database.

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

The temporary password when creating new accounts for systems will be assigned by the IT team member who creates the account.

Note: This addresses PCI requirement 8.2.

3.5.10 Store and transmit only encrypted representation of passw(s)-4.3 (w 0 Tw 42.011(s)-1.4 (p5o4 (p5o4 (

All media containing diagnostic and test programs will go through standard anti-virus scans. University-wide AV policies will scan all media immediately when connected to the system.

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

All remote connections will use standard two-factor authentication to establish VPN connections. IT professionals and 3rd party contractors shall terminate their VPN session as soon as maintenance is complete. VPN connections will automatically disconnect after 30 minutes of inactivity. Also – see section 3.5.6, which requires that 3rd party maintenance accounts be disabled when not in use and monitored when in use.

Note: This addresses PCI requirement 8.3.

3.7.6 Supervise the maintenance activities of maintea70a8(a)-3inac act((e)7.89 (e)-3 b9 (t((e66.6.9 (t((e)7.89 (e

A log shall be maintained in a central location of confidential data being transported outside of normal backup and recovery or other standard business processes that require transport of confidential data. Logging and tracking requirements must be incorporated into standard operating procedures for ongoing transfers of confidential data.

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

All electronic Confidential data shall be encrypted at rest and in transport. Any exceptions must be addressed as a policy exception and explicitly authorized as such.

3.8.7 Control the use of removable media on information system components.

Only AU owned removable media should be attached to AU systems. Removable media containing Confidential data should be encrypted, when possible, and when not, the data itself must be encrypted.

3.8.8

A random sampling of systems will be assessed on an annual basis to evaluate the effectiveness and consistenc of application of the controls defined herein.

NOTE: This control satisfies PCI Requirement #11, Regularly Test Security Systems and Processes.

Derived Security Requirements: None.

3.13 System and Communications Protection

Basic Security Requirements

3.13.1Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

Firewalls shall be in place between the public Internet and all AU systems carrying Internal and Confidential data.
-3 (rn)2.3 ernaB darryC0arryf0.003 darryC0arryotxta3223 (g)11 d-2 (arry)-4.3 (e)7.9.3 (al)1013.3224 0.ryear99 a

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Data stored at rest should be encrypted using AES 256 whenever possible. Standard Microsoft Office encryptio is AES 128 – this is acceptable for temporary storage and transfers of small amounts of confidential data, but for transfer of large amounts of data, Files should be zipped and encrypted using AES 256. For web-based systems, TLS 1.2 encryption should be used, using AES 256 cipher settings.

Exhibit A – Approval of IT Policy Exception

Requestor:	
Date Requested:	Date of request. The approval date is below in the signature section
Policy reference:	Specific policy section to which an exception is being requested
Description of systems or applications impacted:	
Rationale for the exception:	Options may include lack of support from underlying technolog If there are any compensating controls, these should be noted here. here.
Business Risk:	A discussion of the potential impact to confidentiality, integrity or availability of the systems or applications goes here.

[redacted]

Exhibit B - Acknowledgement of Review of 9.3000

The language below shall be used to acknowledge review and acceptance of the 9.3000 policy by