UN Systems Security PCI Policy

POLICY CONTENTS

Scope

This policy applies to all university personnel and entities responsible for managing and supporting Payment Card Industry (PCI)-affected systems. This affects those PCI-identified systems along with campus-wide implemented systems. Those systems that are not centrally managed are to use this policy as best practices for information systems security within their respective information systems environments.

University business units are responsible for following the information security policy development and implementation process established by this policy, communicating their information security policies effectively, reviewing and updating their information security policies regularly, and monitoring their information security policies for compliance and effectiveness.

Policy Statement

Systems Planning, Acceptance, and Operation

Systems Planning
Advanced planning and preparation will be performed to enable the availability of adequate capacity and system resources. Projections of future system capacity requirements will be made to reduce the risk of the system not being able to support processing or storage requirements. The operational requirements of new systems will be established, documented, and tested prior to their acceptance and use.

For major new developments, the operations function and users are to be consulted at appropriate stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests must be carried out to confirm that all acceptance criteria are fully satisfied. The university system development methodology must be followed by applicable parties before a system is implemented in production.

System Acceptance

Acceptance criteria for new information systems handling the transmission of PCI data, significant upgrades, and new versions must be established and suitable tests of the system must be carried out prior to acceptance. System owners working with the appropriate information technology management ensures that the requirements and criteria for acceptance of new systems are clearly defined, agreed upon, documented, and tested. The following controls will be considered:

- Performance and computer capacity requirements
- Error recovery, restart procedures, and contingency plans
- Preparation and testing of routine operating procedures to defined standards
- Agreed set of security controls in place
- Effective manual procedures
- Installation of the new system will not adversely affect existing systems, particularly at peak processing times
- Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:
    - In accordance with PCI DSS (for example, secure authentication and logging)
    - Based on industry standards and/or best practices.
    - Incorporating information security throughout the software-development life cycle
- Address common coding vulnerabilities in software-development processes as follows:

- Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.
- Develop applications based on secure coding guidelines.

Operating Procedures

To ensure the security of the ongoing operation of implemented systems, documented procedures must be created and maintained for system activities associated with systems transmitting PCI data. The operating procedures are in place to ensure that systems are consistently and securely managed. System administrators and system owners are responsible for developing and maintaining operating procedures. Operating procedures are to include affected operating systems such as Windows, Linux, and macOS.

Examples of operating procedures that must be in place for systems include:

- Change management procedures
- Backup procedures
- Job scheduling procedures
- System configuration/security hardening procedures
- System restart and recovery procedures
- Mask access to PAN to no more than first six and last four digits of PAN unless business need to know exists

Such procedures may include those identified by industry practices. Further standards are documented in the Bank Card Handling Procedures.

Configuration

Each PCI related application will be maintained in compliance with the platform security standard for that operating system. This includes but is not limited to:

- Implement only one primary function per server. For example, web servers and data base servers should be implemented on separate servers.
- Virtual servers cannot be utilized unless the virtual host is managed on a separate hypervisor from other non-PCI virtual hosts.
- Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
- Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
- Change vendor-supplied defaults. Remove or disable unnecessary default accounts.
- Encrypt all non-console administrative access to the servers using strong cryptography.
- Maintain an inventory of system components that are in scope for PCI DSS.

System administrators are responsible for ensuring the implementation of an approved security configuration for their associated operating system(s) while Information Security is responsible for the creation and validation of the approved security configuration standard(s). If conflict in a configuration setting exists between the standard(s) and implementation, an appropriate exception request must be filed and documented as an exception to the configuration. Further standards are documented in the Bank Card Handling Procedures.

Vulnerability Management

The university identifies, tracks, and mitigates risks associated with vulnerabilities. Vulnerabilities may be discovered through internal and/or external risk assessment processes, audits, or incidents. System administrators have the responsibility to mitigate all risks associated with a given vulnerability. In the event that a vulnerability may not be mitigated, an appropriate exception must be filed and approved by management. Instructions for vulnerability scans are documented in the bank card handling procedures.

Patch Management

For information systems transmitting cardholder data, all system components and software will be protected from known vulnerabilities by installing applicable vendor-supplied security patches. Critical security patches will be installed within one month of release.

Antivirus (AV)

It is essential that precautions are taken to detect and prevent computer viruses on computers and eradicate them as quickly as possible. Virus protection for all desktop systems and application servers involved in the transmission of PCI data is a requirement for ensuring system uptime and user productivity.

Software

To assure continued uninterrupted service for both computers and networks, all computer users must keep the approved virus detection software enabled on their computers. With virus protection software running, scanning will take place before new data files are opened and before new software is executed. Faculty and staff must not bypass or disable the scanning process since this facilitates the spread or activation of a virus.

For systems considered to be not commonly affected by malicious software, periodic evaluations will be performed to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

AV logs will be generated, and the logs will be retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).

Updates

The antivirus system will provide centralized rapid deployment of virus definition updates. University antivirus systems must be configured to check for the latest version of virus protection on a daily basis.

Non-centralized AV systems

As new versions of the antivirus detection and repair software become available, the product updates are to be distributed to multi-platform computer systems and application servers from the vendor or antivirus servers.

All computers accessible directly from the Internet must run the updated antivirus software.

Virus Detection

For virus-infected systems or suspected virus-infected system, refer to the Digital Security Incident Response Policy.

Backups for Servers

To maintain the integrity and availability of the university's information processing and communication services, routine procedures are established for carrying out the established backup strategy in accordance with business continuity requirements. These procedures include taking backup copies of data and testing their timely restoration, logging events and errors in backups, and, where appropriate, monitoring the equipment environment.

Requirements

To protect university information resources from loss or damage, information owners and custodians are responsible for regularly backing-up their university information. Faculty and/or staff who create and manage critical/regulated data must create the data on appropriate network drives. Network drives provide the necessary backup processes to insure data can be recovered in the event of data loss. Without the data residing on drives which provide a backup process, data could potentially be lost due to errors, omissions, or disk failures.

All backups containing regulated data must be stored at an approved off-site location with either physical access controls or encryption. A contingency plan must be prepared for all applications which handle critical production information. The information owner has the responsibility to verify that the contingency plan is adequately developed, regularly updated, and periodically tested.

Backup copies of essential business information and software are to be taken regularly. Backup copies, accurate and complete records of the backup copies, and documented restoration procedures must be maintained. Adequate backup facilities must be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. A combination of Full backups, Incremental backups, and Differential backups are to be used.

Retention

The retention period for essential information and any requirement for archive copies to be permanently retained must be determined. Information owners are required to identify data that must be kept on a schedule which differs from the standard retention schedule. Some records may need to be securely retained to meet university, statutory, or regulatory requirements, as well as to support essential business activities. A rotation schedule will be established which identifies essential record types, the period of time they are to be retained, and the location where they are stored. Data retention must be conducted in accordance with the university and State of Nebraska Records Retention Guidelines and Policy.

Reason for Policy

The management and operation of the University network information systems must contain controls for the safe transmission and storage of PCI related university information. This policy identifies and defines elements that enable a secure computing systems environment.

Definitions

Virus: An unauthorized program which replicates itself and spreads onto various data storage media (e.g. hard drives, USB sticks, and memory) or across a network, potentially causing damage or compromise to the data or the network. Computer viruses may spread by program files and data files.

Vulnerability: A security weakness or exposure in an operating system or other system software or application software component.

Full Backup: A complete copy of all data to another set of media.

Incremental Backup: A copy only of data that has changed since the last backup of any type.

Differential Backup: A copy only of data that has changed since the last full backup.

Related Information

NU Executive Memorandum 16
NU Executive Memorandum 26
State of Nebraska Consumer Notification of Data Security Breach Act of 2006

This policy covers the following sections of PCI-DSS 3.2:

- 2.1 Change vendor-supplied defaults and remove unnecessary default accounts.
- 2.2 Develop configuration standards for all systems components.
- 2.3 Encrypt all non-console administrative access using strong cryptography.
- 2.4 Maintain an inventory of system components.
- 3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.
- 3.3 Mask PAN when displayed, such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.
- 5.1 Deploy anti-virus software on all systems commonly affected by malicious software.
- 5.2 Ensure that all anti-virus mechanisms are maintained.
- 5.3 Ensure anti-virus mechanisms are actively running and not disabled by users.
- 5.4 Ensure policies and procedures for protecting systems from malware are documented, in use, and known
- 6.1 Establish a process to identify security vulnerabilities.
- 6.2 Ensure all system components and software are protected from known vulnerabilities.
- 6.3 Develop secure software.
- 6.5 Train developers and develop applications based on secure coding guidelines
- 6.7 Ensure policies and procedures for developing security systems are documented, in use, and known
- 10.7 Retain audit trail history.
- 11.2 Run internal and external network vulnerability scans.

History

This policy is a new policy created in 2017.