Technology Help Desk
412 624**-HELP** [4357]
technology.pitt.edu

PAYMENT CARD INDUSTRY TECHNOLOGY GUIDELINES

Introduction

All computers and computer networks handling payment card data must comply with the Payment Card Industry's (PCI) Data Security Standard. Computing Services and Systems Development (CSSD) will assist departments in complying with the requirements of the POLICY, and the guidelines listed below.

In addition to the guidelines below, CSSD provides the following in relation to known systems containing payment card data:

- Maintenance of network diagrams detailing the network data flows and firewall locations.
- Behavioral based intrusion detection.
- Incident response procedures including department coordination and assistance.
- Firewall approval and review procedures to ensure least privilege access is granted and maintained.
- Internal and external vulnerability scanning and management.
- Annual review of PCI system security plans.
- 24/7/365 Monitoring.

Computer System Security

- All systems handling and processing payment card data must be approved by and registered with CSSD.
- A host-based firewall technology must be installed, preventing connections from all ports except a specific subset.
- Anti-virus software must be used daily with up-to-date patches.
- File integrity monitoring to an external system must occur, and logs must be reviewed daily for inappropriate/unauthorized modifications.
- System logging or auditing to an external server for all critical operating system modifications must occur.
- Operating system and application software security patches must remain up to date, with all patches applied within 30 days.
- One primary function per server only must be maintained, and only those services necessary should be enabled.

Connectivity Security

- Servers and workstations must be behind enterprise firewalls to prevent inappropriate/unauthorized access from outside the department or specific authorized computers.
- All Point of Sale devices must be in RFC 1918 private IP space, and not routable directly to the internet.
- CSSD will initiate a semi-annual firewall rule review, and departments must assist in reviewing these rule sets.
- Any data transfers and administrative access must be in an encrypted format.
- All remote access by third-party vendors must be monitored, logged, and only made available on an as-needed basis.

Payment Card Number Storage Requirements

- Credit card numbers must be protected by encryption, hashing, or truncation.
- No complete credit card numbers will be stored on computers in an unprotected manner.
- Copying, moving, or storing credit card numbers on removable electronic media is prohibited unless explicitly authorized by CSSD.

Physical Security

- Servers must be secured in a locked room with access limited to system administrators specially approved for access to credit card numbers or escorted by an employee with access approval.
- All access to servers must be logged.
- Backup media must be secured on site, off site, and in transit with transportation handled by approved employees or bonded couriers.

Audit and Monitoring

- Each department responsible for payment card processing must complete quarterly reviews on all systems storing or processing payment card numbers to ensure they are in compliance with these guidelines and the University's Payment Card Handling and Acceptance Policy.
- CSSD will conduct annual reviews to confirm the results of the departmental reviews, as well as annual risk assessments.
- Departments must also create, maintain, and test business continuity/disaster recovery plans and system compromise response plans annually.
- CSSD will conduct internal quarterly vulnerability scans of all PCI systems, and supply those results to departments. It is the responsibility of the departments to respond to CSSD in a timely manner to resolve any vulnerabilities found.
- CSSD will coordinate external quarterly vulnerability scans of all PCI systems, and supply those results to departments. It is the responsibility of the departments to respond to CSSD in a timely manner to resolve any vulnerabilities found.

Architecture and User Access

- Departments must maintain documented change management procedures in place, and review them on an annual basis.
- Separate testing and development environments must be maintained, and live card holder data cannot be present.
- Separation of duties best practices must be adhered to, where developers do not have access to production systems.
- Access is allowed only by using uniquely assigned and auditable IDs, preferably tied to University central authentication.
- Privileged access to systems must be authorized and approved by a departmental designee, and granted only the level off access required to perform specific job functions.
- Periodic review of all user accounts must be conducted.

Incident Reporting

- In the event of any real or perceived system breach, contact the CSSD Help Desk at 412-624-HELP immediately.