Payment Card Industry Data Security Standard Compliance Policy – Final Draft

Treasury Operations, Updated July 29, 2014

STATEMENT

It is Northwestern University’s intent to protect all Cardholder Data and Sensitive Authentication Data elements from unauthorized access or disclosure, and possible misuse or abuse, throughout the life cycle of the data. This policy addresses the people, processes and controls required to protect cardholder data received, processed, transmitted or stored by, or on behalf of Northwestern University.

Northwestern University credit card merchants must comply with Payment Card Industry Data Security Standards (PCI DSS), must complete annual self-assessment questionnaires, and must attest to their PCI DSS compliance. Merchants shall be responsible for costs associated with PCI DSS compliance as well as any fines or other fees associated with their non-compliance. All Northwestern University employees working with credit cards must read and agree to the conditions of this policy.

The policy applies to cardholder data received, processed, transmitted and/or stored regardless of the processing channel, including but not limited to card swipe terminals, POS systems, e-Commerce/web based applications, virtual terminals, paper forms or facsimile, or telephone.

All individuals involved in the processing of debit and/or credit card payments or who otherwise are exposed to credit and/or debit card information must comply with the Payment Card Industry Data Security Standards. This includes but is not limited to:

- Staff who handle or process debit and credit card payments, or information
- Third parties onsite (e.g. contractors, vendors, business partners, temporary help, etc.) involved in any processing or handling of debit and/or credit card payments, and information
- Technical personnel that maintain or develop systems and solutions used to process cardholder information; this can include security personnel, web administrators, web developers/programmers, and any individual staff responsible for developing, implementing and managing solutions.
GENERAL REQUIREMENTS

All card processing activities and related technologies must comply fully with the Payment Card Industry Data Security Standard (PCI-DSS). Any activity conducted or any technology employed that obstructs compliance with any portion of the PCI-DSS is a violation of this policy and is subject to immediate remedial action. Unless specified otherwise, each of these requirements applies to all merchant card locations.

This policy shall be reviewed annually and updated as needed to reflect changes to business objectives, the risk environment or the applicable standards. Material policy changes will be communicated by email to NU merchants and through ongoing education in self-service or in-person presentation format.

ADDITIONAL GUIDANCE FOR DEPARTMENTS

Each merchant card location is responsible for compliance with PCI DSS. Please pay special attention to the following specific requirements where the department is usually the primary control point. This is not to imply that a merchant can focus on selected requirements, all merchants are required to ensure compliance with all PCI DSS requirements.

NOTE: The specific PCI DSS requirements highlighted below are referenced by the PCI DSS v2.0 requirement numbers enclosed in parenthesis.

(PCI-DSSv2.0 2.1) Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

(PCI-DSSv2.0 2.2.a) Examine the organization’s system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.

(PCI-DSSv2.0 2.2.b) Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.

(PCI-DSSv2.0 2.2.c) Verify that system configuration standards are applied when new systems are configured.

(PCI-DSSv2.0 2.2.3.b) Verify that common security parameter settings are included in the system configuration standards.

(PCI-DSSv2.0 3.1) Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.
(PCIDSSv2.0 3.1.1) Implement a data retention and disposal policy

(PCIDSSv2.0 3.2) Do not store sensitive authentication data after authorization (even if encrypted).

(PCIDSSv2.0 3.3) Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

(PCIDSSv2.0 4.1) Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.

(PCIDSSv2.0 4.2) Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

(PCIDSSv2.0 5.2) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

(PCIDSSv2.0 6.1.b) Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.

(PCIDSSv2.0 6.2) Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

(PCIDSSv2.0 7.1) Limit access to system components and cardholder data to only those individuals whose job requires such access.

(PCIDSSv2.0 8.5.8.b) Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.

(PCIDSSv2.0 9.1) Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

(PCIDSSv2.0 9.7) Maintain strict control over the internal or external distribution of any kind of media.

(PCIDSSv2.0 9.10.1) Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.

(PCIDSSv2.0 9.10.2) Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

(PCIDSSv2.0 11.1) Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

(PCIDSSv2.0 11.2) Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
(PCIDSSv2.0 12.1) Establish, publish, maintain, and disseminate a security policy

(PCIDSSv2.0 12.1.1) Addresses all PCI DSS requirements

(PCIDSSv2.0 12.1.2) Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment

(PCIDSSv2.0 12.1.3) Includes a review at least annually and updates when the environment changes

Policy References


815 ILCS 530 Illinois Personal Information Protection Act (PIPA) of 2006

NU - Related Policies

Retention of University Records

NU Information Technology - Related Policies

NUIT Appropriate Use of Electronic Resources (under review)

NUIT Data Access Policy

NUIT Data Encryption Policy

NUIT Disposal of Northwestern University Computers

NUIT Northwestern University Policy on Wireless Networks

NUIT Secure Handling of Social Security Numbers

Related Guidelines

NUIT Incident Response Protocol

NUIT Contract Language for the Secure Handling of Sensitive Data

NUIT Guidelines for Using Sensitive Data Search Tools
NUIT Mobile Device Security Guidelines

Industry Resources

While the PCI SSC sets the PCI security standards, each of the card brands has its own compliance program, validation levels and enforcement policies. For that reason, please refer to the following links for more payment brand specific compliance information:


Visa Inc. – http://www.visa.com/cisp

Visa Europe – http://www.visaeurope.com/ais

Glossary

**Cardholder Data** – are all identifiable personal data about the cardholder including but not limited to, name, address, telephone number, PAN (#1 above), account expiration date, card security codes (2.a and 2.b above), other data provided by the cardholder, and other electronic data gathered by the applicable merchant or other parties during the course of a transaction.

**Cardholder Data Environment (CDE)** – is defined as the computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment.

**Card Security Code (CSC)** could be either of the following:

- a. The code encoded on the magnetic stripe of a card used for transactions conducted in person. The code ensures that the data stored on the magnetic stripe of the card swiped is valid and was generated by the issuing bank.
- b. The second code, the one most commonly referred to, is the 3 digit code on the back of MasterCard, Visa, and Discover credit or debit cards, to the right of the signature strip; for American Express, it is the 4 digit code that appears above and to the right of the account number. Also known as CVV2, CVC2, CID, CAV2, it is the data used to verify card-not-present transactions.
Credit Card Account Data consists of (but is not limited to):

<table>
<thead>
<tr>
<th>Cardholder Data includes:</th>
<th>Sensitive Authentication Data includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Full magnetic stripe data or equivalent data on a chip</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td>CAV2/CVC2/CVV2/CID</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>PINs/PIN blocks</td>
</tr>
<tr>
<td>Service Code</td>
<td></td>
</tr>
</tbody>
</table>

Payment Card Industry Security Standards Council (PCI SSC) – the standards setting body founded by the payment card brands

PCI DSS Scope – are the system components connected to the CDE; these are governed by PCI DSS and must always conform to the requirements.

PCI-DSS (Payment Card Industry-Data Security Standards) – the set of requirements, published by the PCI council, which govern the behavior of merchants and others who collect cardholder information at the point of sale.

Primary Account Number (PAN) – is the entire credit card account number which is the defining factor in applying PCI DSS requirements. For American Express cards there are 15 digits. For Visa, MasterCard, Discover Card, Diners Club, and JCB there are 16 digits.

Media – refers to all documents whether in paper or any electronic form containing cardholder data. Also refers to devices that can store, process or transmit data such as backup drives, hard drives, removable drives, card swipe terminals, point-of-sale systems