Ecommerce Sites with Redirects to Payment Sites
PCI DSS 3.1 Compliance Checklist
University of Nebraska -Lincoln

June 12, 2015

The University of Nebraska-Lincoln's PCI Team, Bursar's Office and Information Technology Services (ITS) Security, work together to maintain Payment Card Industry Data Security Standards (PCI DSS) for UNL. If a department wishes to accept payment cards, they must comply with UNL's PCI DSS policies and procedures. PCI DSS covers the people, processes, and technology that store, process, or transmit cardholder data. PCI compliance mitigates risk, protects the University against the costs of a breach, and strengthens overall security. When the University complies with PCI DSS, it protects its students, employees, alumni, and customers.

Compliance by all merchants must be achieved and documented annually. Below is a checklist for UNL departments which utilize Ecommerce for payment and allow payment cards.

Table of Contents

Checklist for servers with web redirects:

At implementation:

1) The system administrator or department technical contact is responsible for making sure all merchant applications/systems:
    a. Have changed all vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
        i. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals.
    b. Utilize configuration standards for all system components. ITS has developed best practices (found at http://its.unl.edu/bestpractices)
2) Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.
3) Enable only necessary services, protocols, daemons, etc. as required for the function of the system.
4) Use secure protocols such as SSH, S-FTP, TLS 1.2 for any required services, protocols, or daemons.
5) Encrypt all non-console administrative access using strong cryptography such as VPN, TLS 1.2. (Note: SSL v3 is no longer considered secure.)
6) Remove all unnecessary functionality, such as default scripts, features, and unnecessary web servers.
7) All computer systems in scope will have the UNL anti-virus software deployed and configured for regular updates. AV real-time monitoring must be enabled and logs will be saved for one year.
8) Users accessing systems in scope requiring authentication will use unique User IDs.
9) Strong passwords must be utilized.
10) When remotely accessing systems in scope, the VPN and two factor authentication must be utilized.
11) Implement audit trails (i.e., implement logging) to link all access, events, actions taken and all modifications to all systems in scope. Logs shall be kept for one year.
12) Time settings shall be synchronized by SCCM or Jasper, or by UNL ITS approved time-synchronization technology.
13) Service providers must be vetted through the UNL PCI Team so proper contract wording and the list of service providers is current.

Daily:

1) Logs and security events are to be reviewed at least daily to identify anomalies or suspicious activity.

Quarterly:

1) Monitor user accounts to verify that any inactive user accounts over 90 days old are either removed or disabled.

2) Users accessing systems in scope shall change their password to the system at least once every 90 days, and the password should not use any of the last 4 passwords utilized.

When changes occur:

1) Documentation must be updated when a change is made in system components.
2) Users separated or no longer need access to system components shall be revoked.
3) Vendors needing access to in scope systems will need to be sponsored by the merchant's department, requesting affiliate access. Access is enabled only during the time period needed and disabled when not in use. Vendor's affiliate account will be monitored when in use.
4) Any vulnerabilities identified will be passed to the technical contacts. Vulnerabilities will be patched by the technical contact/system administrator and systems will be re-scanned until the vulnerabilities no longer exist.
5) Any suspected breach of system components in scope are to be promptly reported to the UNL PCI Team via the Security Incident Reporting Form found at http://its.unl.edu/security/security-incident-reporting-form.

Annually:

1) Documentation will be reviewed for modification annually and submitted to the UNL PCI Team.
2) All data flow documentation must include the use of encryption at:
   a. Card swipe
   b. Web redirects
3) Monitor the UNL PCI website for policy change announcements.
4) All personnel working with payment cards will participate in annual cash handling and security awareness training as designed by the UNL PCI Team.

Definitions:

Cardholder Data – At a minimum, cardholder data consists of the full Primary Account Number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

CDE - Acronym for "cardholder data environment." The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.

In-scope – Term used to identify devices that control access to systems which are CDE. CDE and all systems connected to CDE are subject to PCI DSS requirements.

Sensitive Authentication Data - Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

System Components - Any network component, server, or application included in or connected to the cardholder data environment.

PCI DSS Requirements:

Requirement 1 – Install and maintain a firewall configuration to protect cardholder data

1. Firewall changes for systems in-scope for PCI DSS must be requested at http://its.unl.edu/security/firewall-request-form Be specific and detailed in the request.
2. The firewall request will be assessed by the ITS network/information security team. If the request meets the requirements of PCI DSS, the request will be approved. If there are issues with the request, a member of the ITS information security team will be in contact to clarify and amend the request before it is approved.
3. After the change is approved, merchant documentation will be updated by the requestor; network documentation will be updated by the network team.

Requirement 2 – Do not use vendor-supplied defaults for system passwords and other security parameters

1. The system administrator or department technical contact is responsible for making sure all merchant applications/systems:
   a. Have changed all vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.

        i. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals.
    b. Utilize configuration standards for all system components. ITS has developed best practices (found at http://its.unl.edu/bestpractices)
2. Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.
3. Enable only necessary services, protocols, daemons, etc. as required for the function of the system.
4. Use secure protocols such as SSH, S-FTP, TLS 1.2 for any required services, protocols, or daemons.
5. Encrypt all non-console administrative access using strong cryptography such as VPN, TLS 1.2. (Note: SSL v3 is no longer considered secure.)
6. Remove all unnecessary functionality, such as default scripts, features, and unnecessary web servers.

Requirement 3 – Protect stored cardholder data

1. No cardholder data can be stored on UNL servers or networks.

Requirement 4 – Encrypt transmission of cardholder data across open, public networks

1. All data flow documentation must include the use of encryption at:
    a. Card swipe
    b. Web redirects
2. Entering cardholder data on a computer screen from a computer keyboard is prohibited.

Requirement 5 – Protect all systems against malware and regularly update anti-virus software or programs

1. All computer systems in scope will have the UNL anti-virus software deployed and configured for regular updates.
2. All computer systems in scope will have real-time monitor enabled and logs will be saved for one year.

Requirement 6 – Develop and maintain secure systems and applications

1. ITS will monitor various vulnerability and malware announcement sites (such as US CERT). ITS will make announcements to technical contacts about common application vulnerabilities and patching advice. ITS will make announcements regarding latest malware attempts to technical contacts.
2. System administrators and/or departmental technical contacts will apply critical patches within one month of release.
3. Custom software created must follow PCI DSS requirement 6 with supporting documentation.

Requirement 7 – Restrict access to cardholder data by business need to know

1. Cardholder data is not allowed to be stored on UNL systems.

Requirement 8 – Identify and authenticate access to system components

1. Systems in scope should be secured from unauthorized access and logging will be enabled. Logs will be kept for one year.
2. Users accessing systems in scope requiring authentication will use unique User IDs.
3. Users separated or no longer needing access to system components shall be revoked.
4. Monitor user accounts to verify any inactive user accounts over 90 days old are either removed or disabled.
5. Vendors needing access to in scope systems must be sponsored by the merchant's department, requesting affiliate access. Access is enabled only during the time period needed and disabled when not in use. Vendor's affiliate account will be monitored when in use.
6. Strong passwords must be utilized.
7. Users accessing systems in scope shall change their password to the system at least once every 90 days, and the password should not use any of the last 4 passwords utilized.
8. When remotely accessing systems in scope, the VPN and two factor authentication must be utilized.

Requirement 9 – Restrict physical access to cardholder data

1. Cardholder data is not allowed to be stored on UNL systems.

Requirement 10 – Track and monitor all access to network resources and cardholder data

1. Implement audit trails (i.e. implement logging) to link all access, events, actions taken and all modifications to all systems in scope. Logs shall be kept for one year.
2. Time settings shall be synchronized by SCCM or Jasper, or by UNL ITS approved time-synchronization technology.
3. Logs and security events are to be reviewed at least daily to identify anomalies or suspicious activity.

Requirement 11 – Regularly test security systems and processes

1. ITS will run scans for vulnerabilities on all systems in the CDE.
2. An external qualified entity will be hired to perform penetration tests on all systems in the CDE.
3. Any vulnerabilities identified will be passed to the technical contacts. Vulnerabilities will be patched by the technical contact/system administrator and systems will be re-scanned until the vulnerabilities no longer exist.

Requirement 12 – Maintain a policy that addresses information security for all personnel

1. Monitor the UNL PCI website for policy change announcements.
2. All personnel working with payment cards will participate in annual cash handling and security awareness training as designed by the UNL PCI Team.
3. Service providers must be vetted through the UNL PCI Team so proper contract wording and the list of service providers is current.
4. Any suspected breach of system components in scope are to be promptly reported to UNL PCI Team via the Security Incident Reporting Form found at http://its.unl.edu/security/security-incident-reporting-form.