PADSS Implementation Guide

9/25/2015 Blackbaud NetCommunity 4.0 PADSS Implementation US

The information in this manual has been carefully checked and is believed to be accurate. Blackbaud, Inc., assumes no responsibility for any inaccuracies, errors, or omissions in this manual. In no event will Blackbaud, Inc., be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this manual, even if advised of the possibility of damages.

In the interest of continuing product development, Blackbaud, Inc., reserves the right to make improvements in this manual and the products it describes at any time, without notice or obligation.

PADSS-2015

Contents

PA DSS Implementation in Blackbaud NetCommunity

Blackbaud NetCommunity 6 or later, including the current ***6.64***, provides enhancements to help you secure your data and comply with PCI DSS. We strongly recommend you update your software to this version.

Blackbaud Payment Service and Blackbaud NetCommunity

Blackbaud NetCommunity does not store complete credit card numbers in its database. To securely store credit card and merchant account information, ***Blackbaud NetCommunity*** uses the ***Blackbaud Payment Service***. When you update to ***Blackbaud NetCommunity 6*** or later, the program automatically sends your existing credit card information to the web service. If you process credit card payments through ***Blackbaud NetCommunity***, the program uses the ***Blackbaud Payment Service*** to transmit credit card information and process transactions through your merchant accounts. When you first submit credit card information to the ***Blackbaud Payment***

Service for storage, it creates a unique reference number for each credit card number to securely identify and process transactions in accordance with PCI DSS.

In *Administration*, you can manage your login credentials for the ***Blackbaud Payment Service*** from the Configuration page. ***Blackbaud NetCommunity*** uses this information to communicate with the web service.

User Account Security

To comply with PCI DSS, you must change the supervisor login credentials from the default to a unique login name and complex password. We recommend you also change the login credentials of all default user accounts from their default settings and disable any user accounts your organization does not use. In *Administration*, you can edit the login credentials and manage user accounts as necessary.

In *Administration*, you can select to require users to use complex passwords from the System Options page. Complex passwords require at least eight characters, including one upper-case and one lower-case letter and either a special character or number. If you do not select **Require complex passwords**, you must configure the minimum number of characters required and select whether passwords are case-sensitive.

To secure your database, ***Blackbaud NetCommunity*** can automatically lock out a user account after a specified number of failed login attempts. To prevent further attempts, a locked user account remains locked for a specified time period. On the System Options page, you can configure business rules to specify the number of failed attempts to allow before the program locks the user account and the duration of the lockout.

Warning: Do not change the default installation settings for the requirement of unique user login credentials and secure authentication. Adjustment from the default settings and requirements will result in noncompliance with PCI DSS.

For information about additional password and lockout requirements for PCI DSS, see User Account Management on page 9.

Sensitive Authentication Data and Cardholder Data

When you enter new credit card information into ***Blackbaud NetCommunity 6*** or later, the program automatically sends the data to the ***Blackbaud Payment Service*** for storage and retains the reference number generated by the web service. For reference, only the last four digits of the credit card numbers appear in the program.

Note: Prior to version 6, ***Blackbaud NetCommunity*** stored unencrypted cardholder data. After you update to ***Blackbaud NetCommunity 6*** or later, the program securely deletes cardholder data and sends it to the ***Blackbaud Payment Service*** for storage. Since ***Blackbaud NetCommunity 6*** or later does not store cardholder data, there is no cardholder data to securely purge as required by PA DSS requirement 2.1. No previous versions of ***Blackbaud NetCommunity*** used encryption; therefore, there is no cryptographic data to securely remove as required by PA DSS requirement 2.7.

When website users enter new credit card information through your website, such as through a donation form, the program automatically sends the data to the ***Blackbaud Payment Service*** for storage and retains the reference number generated by the web service. The user can only access the credit card information entered during the same session on your website.

Your organization can use attributes, notes, and free-text fields to store important information. However, do not use these features to store information such as sensitive authentication data or cardholder data in the program. The abuse or misuse of the program to store this information can leave you vulnerable to an attack by malicious users. If your organization used attributes, notes, or free-text fields to store sensitive authentication data or cardholder data, you must securely delete this data from your database to comply with PCI DSS. For information about how to delete this data, see Sensitive Authentication Data and Cardholder Data Retention on page 8.

Blackbaud NetCommunity does not facilitate the transmission of primary account numbers (PANs) through messaging technology such as email or instant messages. For information about the transmission of cardholder data over open public networks, see Cardholder Data Encryption on page 9.

Merchant Accounts

Blackbaud NetCommunity does not store decrypted login credentials for merchant accounts in the database. The program uses the ***Blackbaud Payment Service*** to store your organization's merchant account information. ***Blackbaud NetCommunity*** can retrieve your merchant account information from the ***Blackbaud Payment Service***.

Website Design

The Frame part and the News Reader part and page element can retrieve information from potentially unverified third-party sources. To comply with PCI DSS, do not use these parts if they reference third-party websites your organization does not trust or cannot verify.

In *Administration*, on the System Options page, you can select the HTML elements to allow in the client-facing HTML editors. To comply with PCI DSS, we recommend you not select **IFRAME** or **SCRIPT** to prevent the use of these tags from within your website.

Integration with The Raiser's Edge

Blackbaud NetCommunity does not send decrypted credit card numbers to ***The Raiser's Edge***. When the program sends transaction information, it includes the reference number generated by the ***Blackbaud Payment Service***. ***The Raiser's Edge*** uses this reference number to identify the credit card number.

To process a donation or membership transaction that includes recurring gift information, you must use ***The Raiser's Edge 7.91*** or later.

Rollback and Uninstall

Before you install any updates, we strongly recommend you back up your database. For information about the update process, see the *Update and New Features Guide*.

If you encounter problems during the installation process, you can cancel the installation before it finishes. After you cancel, the install utility returns your machine to its state before the installation. If you complete the installation process but feel the program may have installed improperly, you can sue the **Add or Remove Programs** utility, available from the Control Panel in *Windows*-based operating systems, to safely uninstall the application.

All installation and update guides are available from the user guides area of our website at https://www.blackbaud.com/support/guides/guides.aspx.

Services and Protocols

Blackbaud NetCommunity does not require the use of any insecure services or protocols. The services and protocols that ***Blackbaud NetCommunity*** requires are Secure Sockets Layer (SSL) v3 and Hypertext Transfer Protocol Secure (HTTPS). For information about SSL, see Secure Sockets Layer Configuration on page 4.

Secure Sockets Layer Configuration

Secure Sockets Layer (SSL) is a protocol developed by Netscape to transmit private documents via the Internet. SSL uses a public key to encrypt data transferred over a SSL connection. Microsoft *Internet Explorer* and other browsers support SSL. ***Blackbaud NetCommunity*** permits use of the protocol to safely transmit confidential information such as credit card numbers and login information.

To ensure sensitive data is secure over the Internet, you must enable SSL for ***Blackbaud NetCommunity***. To that end, it is important you understand the steps necessary to set up SSL.

Digital Certificates in Internet Information Server

After you acquire a digital certificate, configure it on your NetCommunity web server in *Internet Information Server (IIS)*. To add the new certificate to your web server, follow the directions from Microsoft located at http://support.microsoft.com/kb/228836/. The digital certificate provides the public key that SSL needs to encrypt data. When Blackbaud hosts ***Blackbaud NetCommunity***, the installation engineer assists in the process. For information about how to obtain a digital certificate, see the ***Blackbaud NetCommunity*** System FAQs document provided by Blackbaud Professional Services.

Digital certificates relate to only one root domain name, not an IP address or specific server. For example, you do not need to acquire a certificate for http://www.mydomain.com/netcommunity. Instead, acquire the certificate only for www.mydomain.com. Additionally, when you configure your digital certificate on your default website, do not set the **Require secure channel (SSL)** option in *IIS*. This unnecessarily enables SSL across your entire website.

Configure SSL in Blackbaud NetCommunity

To install ***Blackbaud NetCommunity***, Blackbaud Professional Services follows a series of procedures. If you request that Professional Services enable SSL during your initial implementation, they use these steps. If you do not request Professional Services' assistance, you must complete these on your own.

- After the installation, from *Configuration*, specify whether to require SSL on all pages of your website or only the Administrative site or pages on the Client site that contain sensitive information.
- In *IIS*, the SSLPage.aspx in the NetCommunity virtual directory is modified. This is the only in the instance security settings for the SSL certificate are set to **Require Secure Channel (SSL)**.
- If Blackbaud hosts ***Blackbaud NetCommunity*** for you and your web service is located on your web server in the hosted environment, it must be secure. This requires a separate digital certificate on that web server for its domain. This is documented in theTechnical Requirements document provided by Blackbaud Professional Services. Additionally, when Blackbaud hosts ***Blackbaud NetCommunity***, Professional Services configures a digital certificate on the NetCommunity web server for your domain.

SSL in Blackbaud NetCommunity

By default, when you enable SSL in ***Blackbaud NetCommunity***, only selected parts are enabled to use SSL. These parts include the User Login, Donation Form, Membership Form, Event Registration Form, Fundraiser, Formatted Text and Images (Secured), and Personal Page Manager. If you set the **RequiresSSL** field to 1 in the **ContentTypes** table in your ***Blackbaud NetCommunity*** database, you can add additional parts as secured.

To secure multiple pages on your website, add an empty Formatted Text and Images (Secured) part to any layout in ***Blackbaud NetCommunity***. This way, any web page that uses the layout is automatically secured.

When a website user is on a page that has a secured part, ***Blackbaud NetCommunity*** dynamically configures each image URL, URLs defined in parts, and document file URLs to "https". When a user navigates to any one page that contains an SSL part, the small lock appears on the browser. ***Blackbaud NetCommunity*** maintains this secured environment to the next page the user navigates to. It does not matter whether it has an SSL-enabled part. Any data transmitted from these secured pages is encrypted.

Configure SSL Settings in the Windows Registry

Warning: If you modify the registry file incorrectly, serious problems may occur. Before you edit the registry, we strongly recommend you create a backup so you can restore the file if necessary. For information about how to back up and restore the registry file, see http://support.microsoft.com/kb/322756.

To ensure the safe transfer of sensitive credit card data from ***Blackbaud NetCommunity***, you must configure your SSL settings to enforce strong encryption. To prevent the weak encryption of credit card information, edit these SCHANNEL keys in your *Windows* registry panel:

```
[HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]
“Enabled”=dword:00000000

[HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40\128]
“Enabled”=dword:00000000

[HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56\128]
“Enabled”=dword:00000000

[HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]
“Enabled”=dword:00000000
```

For more information about how to adjust the Schannel.dll file to restrict cryptography and protocols, see http://support.microsoft.com/kb/245030.

Additional SSL Information

To avoid mixing secure domains with non-secure content, you must modify ***Blackbaud NetCommunity*** background URLs on Menu parts or in your custom CSS to "https://" (instead of "http://"). In addition, we recommend you modify any javascript URLs used in Formatted Text and Images parts to "https://".

In these situations, you can set URLs used to relative URLs. For example, for background images in your styles view.image?Id= 478 in the URL can be used in a style, such as background-image:url (view.image?Id= 478);. In this example, the URL references an image in *Images*. This is resolved to the correct domain during rendering, regardless of security.

We recommend that you sparingly use fixed URLs in styles and javascript because SSL retrieves the images every time it loads a fixed page. It does not matter whether the page is secure.

If you do not enable SSL on the ***Blackbaud NetCommunity*** Administrative site, but you do enable the client site web pages, mixed mode messages and SSL redirect messages may appear when you switch between administration pages and your website pages.

If you plan to host objects such as streaming media files or iframes that reference files hosted elsewhere, we recommend you consider the issue of combining secure and non-secure content. A non-secure page in an iframe on the same page as a secured ***Blackbaud NetCommunity*** web page is considered mixed content. In each instance, during the design of your site, we recommend you located mixed areas of content together on the same NetCommunity web server or secured by its own digital certificate.

PCI DSS Implementation

When you accept payment cards for donations or revenue, the security of the credit card information is very important. Used properly, Blackbaud programs can help you maintain this information in accordance with the Payment Card Industry Data Security Standard (PCI DSS). To help promote this awareness of the security requirements for credit card and cardholder data, this chapter provides information about PCI DSS and how it impacts your organization. With the proper security of credit card information, you can protect your constituents and clients from inconvenience and financial and personal loss, and help protect your organization from additional expense.

Note: This guide provides only an overview of PCI DSS requirements and recommended best practices to ensure compliance. For additional detail, visit https://www.pcisecuritystandards.org to download the PCI DSS specification.

Payment Card Industry and Payment Application Data Security Standards

Developed by Visa, the Payment Application Data Security Standard (PA DSS) requires software companies such as Blackbaud to develop secure programs that enable users to comply with the PCI DSS. To learn more about PA DSS and download the specification, visit http://usa.visa.com/download/merchants/cisp_payment_application_best_practices.doc.

Note: The Payment Card Industry (PCI) Security Standards Council includes American Express, Discover Financial Services, JCB International, Mastercard Worldwide, and Visa Inc. and was formed to help implement consistent data security measures on a global basis.

Developed by the PCI Security Standards Council, the PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other proactive measures. As an organization that collects payment card information, such as to process payments or donations, you must adhere to the PCI DSS and proactively protect this data. To learn more about PCI DSS and download the specification and its supporting documents, visit https://www.pcisecuritystandards.org.

Note: Depending on your organization and the number of payment card transactions you process, you may need to engage an external security assessment company to determine your level of compliance with PCI DSS and other security compliance programs. If you use an external assessor, we recommend you select one that is qualified and familiar with the latest requirements from the PCI Security Standards Council. To validate whether your organization is compliant with PCI DSS, we recommend you also visit https://www.pcisecuritystandards.org and complete the PCI Security Standards Council Self-Assessment Questionnaire.

Data Management

Encryption is necessary to protect cardholder data. If a user circumvents security controls and gains access to encrypted data, without the proper cryptographic keys, the user cannot read or use the data. To reduce the risk of malicious abuse, you must consider other effective methods to protect stored data. For example, store cardholder data only when it is absolutely necessary, and do not send the cardholder data in unencrypted email messages.

Sensitive Authentication Data and Cardholder Data Retention

You should keep the storage of cardholder data to a minimum. To comply with PCI DSS, your organization must develop and maintain a data retention and disposal policy.

- Limit the cardholder data stored and the retention time to only that which is required for business, legal, and regulatory purposes.
- Purge all cardholder data that exceeds the retention period.

Do not retain sensitive authentication data, such as the full magnetic stripe, card validation code, or personal identification number (PIN) information, in your database. If you must retain sensitive authentication data, such as for troubleshooting purposes, you must follow these guidelines:

- Collect sensitive authentication data only when necessary to solve a specific problem.
- Store sensitive authentication data only in specific, known locations with limited access.
- Collect only the limited amount of data necessary to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete sensitive authentication data after use.

Warning: To comply with PCI DSS, you must remove historical sensitive authentication data and cardholder data from your database. If you upgrade from a non-compliant version, or if your organization used attributes, notes, or text-free fields to store sensitive authentication information or cardholder data, you must search for and securely delete this data from your database to comply with PCI DSS.

To ensure the complete and secure removal of cardholder data, you must securely erase temporary files that may contain sensitive authentication information and cardholder data.

- If you use Microsoft *Windows XP* or *Windows Vista*, turn off System Restore on the System Properties screen. To track changes in *Windows*, System Restore creates and uses restore points, which may retain cardholder data. When you turn off System Restore, the operating system automatically removes existing restore points and stops the creation of new restore points.
- To ensure the complete removal of data, install and run a secure delete tool such as Heidi *Eraser*. With a secure delete tool, you can safely erase temporary files that may contain sensitive information or

cardholder data. For information about how to install and run the secure delete tool, refer to the manufacturer's documentation.

Cardholder Data Encryption

To comply with PCI DSS, your organization must encrypt cardholder information during transmission over open public networks that malicious users could abuse to intercept, modify, and divert data during transit. These open public networks include the Internet, WiFi (IEEE 802.11x), the global system for mobile communication (GSM), and general packet radio service (GPRS). To safeguard sensitive authentication information and cardholder data during transmission, use strong cryptography and security protocols such as Transport Layer Security (TLS) version 1.0 (or above) and Internet Protocol Security (IPSEC). Never send unencrypted cardholder data in an email message.

Network Security

With a secure network, you can protect your system and credit card information from internal and external malicious users. To secure your network, we recommend you utilize a firewall and configure wireless devices and remote access software.

User Account Management

To comply with PCI DSS, you must assign unique identification to each person who accesses networks, workstations, or servers that contain the program or cardholder data. Unique login credentials ensure that only authorized users can access and work with the critical data and systems included in your network. With unique login credentials, you can also trace actions on your network to specific users. These credentials must include a unique user name and a way to authenticate the user's identity, such as a complex password, a token key, or biometrics.

At a minimum, your organization must implement these guidelines to create network user accounts and manage user authentication and passwords. You must communicate password procedures and policies to all users who can access cardholder data.

- Use authorization forms to control the addition, deletion, and modification of user IDs.
- Verify the identity of users before you reset passwords.
- Immediately revoke account access for terminated users.
- Remove or disable inactive user accounts at least every 90 days.
- Enable user accounts for use by vendors for remote maintenance only when needed, and immediately deactivate them after use.
- Do not use group, shared, or generic user accounts and passwords.
- Require users to change their initial passwords immediately after the first use and subsequent passwords at least every 90 days.
- Require passwords with a minimum length of seven numeric and alphabetic characters.
- Require that new passwords not match one of the last four passwords used by the user.
- Lock out the user account after no more than six failed login attempts. Set the lockout duration to 30

minutes or until a system administrator enables the user account.

- Log out idle sessions after 15 minutes so users must enter the password to activate the workstation.
- To log user authentication and requests, turn on database logging in Microsoft *SQL Server*.

Firewall Management

If you use software to process payments, we recommend you verify that the workstation's link to the Internet is secure. If you transfer transactions online, ensure your Internet hardware, such as the modem or DSL router, provides a built-in firewall. You must restrict connections between publicly accessible servers and any system component that stores cardholder data, including connections from wireless networks. To comply with PCI DSS, the firewall configuration must:

- Restrict inbound Internet traffic to Internet Protocol (IP) addresses within the DMZ.
- Not allow internal addresses to pass from the Internet into the DMZ.
- Implement inspection or dynamic packet filtering to allow only established connections into the network.
- Place the payment processing program and the database that contains the cardholder data in an internal network zone segregated from the DMZ.
- Restrict inbound and outbound traffic to only that which is necessary for the cardholder data environment, and deny all other traffic that is not specifically allowed.
- Secure and synchronize router configuration files such as running and start-up configuration files.

Your organization must also install perimeter firewalls between any wireless networks and the cardholder data environment and configure these firewalls to deny or control any traffic from the wireless environment. To comply with PCI DSS, your organization must configure all mobile and employee-owned computers with direct connectivity to the Internet, such as laptop computers, used to access the network with an installation of personal firewall software.

Wireless Devices

If you use wireless devices to store or transmit payment transaction information, you must configure these devices to ensure network security in compliance with PCI DSS.

- Install perimeter firewalls between any wireless networks and systems that store cardholder data. These firewalls must deny or control any traffic necessary for business purposes from the wireless environment to the cardholder data environment.
- Implement strong encryption, such as Advanced Encryption Standard (AES), on all wireless networks.
- At installation, change wireless encryption keys, passwords, and SNMP community strings from the default. After installation, change wireless encryption keys, passwords, and SNMP community strings when anyone with knowledge of these items leaves the organization or changes positions with the organization.
- Do not use the vendor-supplied defaults for the wireless environment. Change the default passwords or pass phrases on access points and single network management protocol (SNMP) community strings on wireless devices.
- Change the default service set identifier (SSID) and disable SSID broadcasts when applicable.
- Update the firmware on wireless devices to support strong encryption—such as WiFi-protected access

(WPA or WPA2) technology, Internet Protocol security virtual private network (IPSec VPN), or Transport Layer Security (TLS)—for authentication and transmission over wireless networks.

- Use industry best practices (for example, IEEE 802.11i) to implement strong encryption for the transmission of cardholder data and sensitive authentication data over the wireless network in the cardholder data environment.

Warning: As of June 30, 2010, it is prohibited to use Wired Equivalent Privacy (WEP) for payment applications. We strongly recommend you use WPA2 technology to secure wireless implementations.

To comply with PCI DSS, your organization must configure all mobile and employee-owned computers with direct connectivity to the Internet, such as laptop computers, used to access the network with an installation of personal firewall software. The firewalls must be active and configured to a specific standard that users cannot alter.

Remote Access

Blackbaud CRM payment functionality is accessible only to users with access to your organization's network. The application is configured to only be accessible with network access by default. Blackbaud does not have nor require access to customer networks in order to install ***Blackbaud CRM***. ***Blackbaud CRM*** updates are not delivered via remote access from Blackbaud.

If your organization allows for remote network access by employees, administration, and vendors, you must implement two-factor authentication (T-FA) for logins in order to meet PCI-DSS requirements. T-FA requires unique login credentials (username and password) and an additional authentication item such as a token or individual certificate. Use of technology such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens or VPN (based on TLS or IPSec) with individual certificates are acceptable methods of T-FA.

To comply with PCI DSS, your organization must configure the remote access software to ensure network security.

- Do not use the vendor-supplied defaults, such as passwords, for the remote access software.
- Establish unique login credentials and complex passwords for remote access users in accordance with PCI DSS requirements 8.1.5 and 8.3. For information, see User Account Management on page 9.
- Allow connections from only specific known IP and MAC addresses.
- Enable encrypted data transmission in accordance with PCI DSS 4.1.
- Lock out the remote access user account after no more than six failed login attempts.
- Require remote access users to establish a VPN connection through a firewall before they connect to the network.
- Enable the logging function.
- Establish complex passwords for customers in accordance with PCI DSS requirements 8.2.3.
- Restrict access to customer passwords to authorized third-party personnel.
- To verify the identities of remote access users, require T-FA such as both a user login and a password.

If your organization enables remote access for use by vendors, it should be only when needed and immediately deactivated after use.

Non-console Administrative Access

To comply with PCI DSS, your organization must encrypt all non-console administrative access. For web-based management and other non-console administrative access, use technologies such as Secure Shell (SSH), VPN, or TLS.

If you use Remote Desktop (RDP) for non-console administrative access, it is advised that you follow best practices for RDP security such as digitally signing RDP files with a custom certificate, tightening connection security through a TLS security layer and raising the encryption level to high, and using network level authentication.

For information on configuring RDP security, see Microsoft documentation at https://technet.microsoft.com/en-us/library/cc753488.aspx.

Internet-Accessible Systems

Do not store cardholder data on Internet-accessible systems. For example, do not house the database server within the same server as the web server.

System Maintenance

Once you secure your system, you must keep your equipment current. Malicious users can use security vulnerabilities to access your system. Both hardware and software manufacturers occasionally issue updates to products, such as to remedy these vulnerabilities and help prevent such attacks. We recommend you ensure you have the most recently released patches installed. For example, you can frequently review the manufacturer's websites, newsletters, and online forums to check for the current patches.

Occasionally, a manufacturer may stop support of a product. In this case, we recommend you determine whether your organization should continue to use an unsupported product. Also, a manufacturer may inform you of a flaw or defect in a product that may make your organization vulnerable to attack. We recommend you pay attention to these alerts and update your system accordingly.

To further reduce vulnerability, we recommend you also deploy anti-virus software on your systems and ensure they are current, actively running, and can generate assessment logs.

Network Maintenance

Once you secure your system, you must monitor and track access to the network and your credit card information, such as with logging mechanisms. The lack of activity logs can make the determination of the cause of an attack very difficult. Logs help you track and analyze network activity when something goes wrong. To further reduce vulnerability, we recommend you also frequently test your network to verify its security continues to be maintained, regardless of age or changes in software.

To comply with PCI DSS, you must implement automated audit trails for all system components to track these events:

- All individual users who access cardholder data.
- All actions performed by users with root or administrative privileges.
- All access of the audit trails.
- All invalid logical access attempts.

- All use of identification and authentication mechanisms.
- The initialization of the audit logs.
- The creation and deletion of system-level objects.

For each event, your organization must also record these audit trail entries for all system components:

- The user who initiates the event.
- The type of event.
- The date and time of the event.
- Whether the event succeeds or fails.
- The origination of the event.
- The data, system component, or resource the event affects.

Revision Information

This guide is reviewed and updated as necessary on a yearly basis and based on changes to ***Blackbaud NetCommunity*** or the PCI DSS and PA DSS specifications. Blackbaud distributes this guide through the user guides page on our website at https://www.blackbaud.com/support/guides/guides.aspx.

Author	Revision date	Summary of changes
Steve Stegelin (Technical Writer III)	March 2009	
Steve Stegelin (Senior Technical Writer)	January 2011	Update document template.
Steve Stegelin (Information Architect)	June 2012	Add this table; Update document template; minor edit to remove recent-speaking terms such as "now" and "new".
Steve Stegelin (Information Architect)	October 2012	Reversed order of chapters; updated index to reflect PA DSS 2.0; added Services and Protocols on page 4; updated Sensitive Authentication Data and Cardholder Data on page 2
Steve Stegelin (Information Architect)	July 2014	Update version number to include ***6.58***.
Britt Murray (Staff Technical Writer)	September 2015	Update version number to ***6.64***.

Index