Chargepath
PA-DSS Implementation Guide

This guide was produced to help you securely implement Chargepath credit card processing software in your business. It is important that you read and understand this document to help you secure your customers' credit card data.

About Chargepath

Chargepath is credit card processing software designed as an integrated credit card processing component to work with business software like point of sale and accounting systems. Chargepath processes credit card transactions through Mercury Payment Systems or with PCCharge Payment Server.

Chargepath handles sensitive credit card data, delivering that information to Mercury's software on your local network. Mercury's software communicates the credit card information, receives the authorization result, and returns that to Chargepath. Chargepath works similarly with PCCharge Payment Server when processing credit cards with processors other than Mercury Payment Systems.

About the PCI Security Standards

The PCI DSS (Payment Card Industry Data Security Standard) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. All businesses handling credit and debit cards are required by the card brands to maintain PCI DSS compliance.

The PA-DSS is a security standard designed to help software vendors develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI Data Security Standard. All payment applications handling credit and debit cards are required by the card brands to maintain PA-DSS compliance.

Part of your responsibility in complying with the security standards includes using PA-DSS Validated software. Chargepath handles this for you. The remaining steps for compliance are detailed in this guide and involve the way your computers and network are set up, maintained and used. Both of these are required for you to comply with the requirements of the security standards.

For more information on the PCI standards, visit http://www.pcisecuritystandards.org

Software License and Limited Warranty

This Inborne Technology Corporation End-User License Agreement ("EULA") is a legal agreement for the Inborne Technology Corporation Software Product in which this EULA is contained, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (collectively the "Software Product"), between you and Inborne Technology Corporation. By installing, copying, or otherwise using the Software Product, you agree to be bound by the terms of this EULA. You must indicate your agreement to be bound by the terms of this EULA by pressing the "I ACCEPT" button on the Software Product's installation program, or else you will not be able to install the Software Product. If you do not agree to the terms of this EULA, you may not install or use the Software Product; you may, however, within 30 days of your initial purchase of a copy of the Software Product, return the entire copy of the Software Product (including all computer media, packaging and documentation) either to Inborne Technology Corporation's Customer Service department or to the retailer from which you purchased the Software Product, for a refund of the amount indicated by your sales receipt for the Software Product, in which event your rights under this EULA are immediately terminated. If you are installing the Software Product on a computer that is not owned by you, you are bound to the terms of this EULA both in your individual capacity and as an agent of the owner of the computer, and your actions will bind the owner of the computer. You represent and warrant to Inborne Technology Corporation that you have the capacity and authority to enter into this Agreement on your own behalf as well as on behalf of the owner of the computer the Software Product is being installed upon. For purposes of this EULA, the "owner" of a computer is the individual or entity that has legal title to the computer or that has the possessory interest in the computer if it is leased or loaned by the actual title owner.

COPYRIGHT. The Software Product is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. All title and copyrights in and to the Software Product (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the Software Product) are owned by Inborne Technology Corporation or its suppliers.

GRANT OF LICENSE. The Software Product is licensed, not sold. Subject to the condition that you are in compliance with the terms of this EULA: (a) you may install and use one copy of the Software Product, or any prior version for the same operating system, on a single computer for use by a single simultaneous operator; and (b) you may install a single copy of the Software Product, strictly for your own personal use, on one portable computer owned by you. No other use, copying or distribution of the Software Product is permitted. You may not rent the Software Product, nor may you offer use of it to others through a service bureau or application service provider. If you are installing this copy of the Software Product as an upgrade, update, patch or enhancement of a prior release of the same Software Product which was installed on the same computer, your rights under the prior license agreement for the Software Product are terminated, and all of your use of the Software Product (including its prior versions) are solely under the terms of this license agreement.

LIMITATIONS. Except to the extent such a restriction is unenforceable under local law, you may not reverse engineer, decompile, or disassemble the Software Product. The Software Product is licensed as a single product, and its component parts may not be separated for use on more than one computer. You may not modify, amend, or create derivative works of the Software Product.

TERM. The licenses granted under this EULA commence upon the installation of the Software Product and are effective in perpetuity unless terminated per the terms of this Agreement.

TERMINATION. Without prejudice to any other rights, Inborne Technology Corporation may terminate this EULA or your rights under this EULA at any time if you fail to comply with the terms and conditions of this EULA. Upon termination of your rights under this EULA for any reason, or upon termination of the EULA itself, you must destroy all copies of the Software Product and all of its component parts in your possession (including all component parts, the media and printed materials, any prior versions, and this EULA). The terms of this paragraph shall survive any termination of this EULA.

TRANSFER. You may permanently transfer all of your rights under this EULA, provided you retain no copies, you transfer all copies of the Software Product (including all component parts, the media and printed materials, any prior versions, and this EULA), and the recipient agrees to be subject to the terms of this EULA. Upon the occurrence of such a transfer, your rights under this EULA terminate immediately.

LIMITED WARRANTY. The warranties and disclaimers described in this paragraph are collectively the "Limited Warranty". Inborne Technology Corporation warrants to you (and only you) that the Software Product will perform substantially in accordance with the accompanying documentation (if any) for a period of ninety (90) days from the date of original purchase of a license to the Software Product from an authorized retailer or directly from Inborne Technology Corporation (in each case the "Purchase Date"). Implied warranties on the Software Product, to the extent required by applicable law, are limited to ninety (90) days from the Purchase Date. Some states do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, INBORNE TECHNOLOGY CORPORATION AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS WITH REGARD TO OR ARISING OUT OF THE SOFTWARE PRODUCT, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT

LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND/OR ACCURACY OF INFORMATION. The Limited Warranty is void if failure of the Software Product has resulted from accident, abuse, misapplication, use of the Software Product other than as described in the documentation issued by Inborne Technology Corporation, use of the Software Product in combination with other Software Products that are not described as compatible in the documentation issued by Inborne Technology Corporation, or your breach of the terms of this EULA. This warranty gives you specific legal rights, and you may also have other rights which vary from State to State. No individual (except a duly authorized officer of Inborne Technology Corporation) and no reseller or retailer has any authority to amend or add to any of the above representations and disclaimers.

YOUR REMEDY. Your exclusive remedy for any breach of the Limited Warranty is for you to give us notice of the breach by returning to Inborne Technology Corporation (at the address shown below) a copy of your purchase receipt for your copy of the Software Product and a description of the alleged breach, and then, at Inborne Technology Corporation's option, Inborne Technology Corporation shall either: (a) return the price you paid (if any) for the Software Product (at which time your rights under this EULA are deemed to have terminated); or (b) repair or replace the Software Product. The Limited Warranty period for any replacement Software Product will be extended for the remainder of the original warranty period or thirty (30) days after the replacement Software Product is delivered to you, whichever is longer. Your remedies described in this paragraph are your exclusive remedies, and shall not be deemed to fail of their essential purpose so long as Inborne Technology Corporation is willing to repair or replace the Software Product or return the price you paid for the Software Product.

LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL INBORNE TECHNOLOGY CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF INBORNE TECHNOLOGY CORPORATION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, INBORNE TECHNOLOGY CORPORATION'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS EULA SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR US$5.00. Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

THIRD PARTY WORKS. To the extent that any third party's intellectual property is incorporated within the Software Product, you agree that such third party is a third-party beneficiary of the terms of this EULA to the extent of the third party's license to Inborne Technology Corporation.

GENERAL. This EULA constitutes the entire agreement between you and Inborne Technology Corporation concerning the Software Product. No terms of any purchase order, acceptance, purported amendment, or any document or communication other than an agreement expressly agreed upon in writing by a duly authorized officer of Inborne Technology Corporation shall replace, modify, amend or override this EULA. If any provision of this EULA is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable, and such decision shall not affect the enforceability of such provision under other circumstances, or of the remaining provisions hereof under all circumstances. No waiver by Inborne Technology Corporation of any breach of any term or provision of this EULA shall be construed to be a waiver of any preceding or succeeding breach of the same or any other term or provision hereof. Our various rights and remedies hereunder shall be construed to be cumulative and no one of them is exclusive of any other or of any right or remedy allowed by law or in equity. This EULA shall be governed by and construed in accordance with the laws of the State of Arizona, USA (without regard to its choice of law principles), except to the extent the local law of your local jurisdiction requires use of your local jurisdiction's law, and shall benefit Inborne Technology Corporation, its successors and assigns. ANY CLAIM OR DISPUTE BETWEEN YOU AND INBORNE TECHNOLOGY CORPORATION OR AGAINST ANY AGENT, EMPLOYEE, SUCCESSOR OR ASSIGNEE OF INBORNE TECHNOLOGY CORPORATION, WHETHER RELATED TO THIS AGREEMENT OR OTHERWISE, AND ANY CLAIM OR DISPUTE RELATED TO THIS AGREEMENT OR THE RELATIONSHIP OR DUTIES CONTEMPLATED UNDER THIS AGREEMENT, INCLUDING THE VALIDITY OF THIS ARBITRATION CLAUSE, SHALL BE RESOLVED BY BINDING ARBITRATION BY THE NATIONAL ARBITRATION FORUM TO BE HELD IN PHOENIX, ARIZONA UNDER ITS CODE OF PROCEDURE THEN IN EFFECT. Any award of the arbitrator(s) may be entered as a judgment in any court of competent jurisdiction. Except as may be required by law, neither a party nor an arbitrator may disclose the existence, content, or results of any arbitration hereunder without the prior written consent of both parties. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this EULA. Should you have any questions concerning this EULA, or if you desire to contact Inborne Technology Corporation for any reason, please contact: Inborne Technology Corporation, 916 E. Baseline Rd., Suite 132, Mesa, Arizona, 85204 USA/Telephone: (480) 497-4004/Facsimile: (480) 497-2442.

Steps to ensure that your system is secure

Implementing Chargepath Securely

Of the PA-DSS and PCI DSS criteria that determine the security level and ultimate compliance of your system, these areas stand out as requiring particularly close attention:

- Storing card data
- Encryption of data over public networks
- Remote access
- Wireless network considerations
- Network setup and segmentation
- User management
- Logging
- Virus/malware protection and firewall

Storing Sensitive Card Data

Chargepath will never store any card data. There are no debugging or troubleshooting settings in the software that permit sensitive data to be stored. Storing sensitive card data through alternate means like entering a card number in a customer account contact field or note must be avoided.

To keep credit card data secure you must not allow credit card data to be transferred through email or messaging systems like instant messages or SMS text messages. Additionally, you must not store credit card data in any other software (like word processing, database or spreadsheet programs).

Encrypt Sensitive Traffic over Public Networks

Chargepath hands off credit card data to Mercury Payment Systems Datacap DSIClientX or PCCharge Payment Server software to send transactions containing card data over the Internet for processing. All cardholder data is securely encrypted using an approved strong encryption technology before it leaves your system for processing.

Chargepath is incapable of sending unsecured cardholder data over the Internet (public network). Attempting to send sensitive card data through alternate means like email, instant messaging or text messaging must be avoided to minimize risk of cardholder data theft and to meet credit card data security requirements.

Remote Access

Chargepath does not require the use of remote access or any other form of remote administration. If you use an alternate administration interface (*e.g.* Remote Desktop, LogMeIn, GoToMyPC, CrossLoop) to access your payment processing environment or to make administrative changes in Chargepath, the traffic must be encrypted with a secure encryption technology (*e.g.* SSH, VPN, or SSL/TLS) to maintain credit card data security compliance.

- Do not use remote access solutions requiring “port forwarding” such as VNC and PCAnywhere.

- Use two-factor authentication for remote access. Use technologies such as RADIUS, TACACS with tokens, or VPN with individual certificates assigned to each user. Two-factor authentication means that two of the following three things are required: Something the user **knows** (like a password), something the user **has** (like a one-time use key) or something the user **is** (like biometric data).

- Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:

  - Explicit management approval to connect any device to your network
  - Authentication for use of the technology
  - A list of all such devices and personnel with access
  - Labeling of devices with owner, contact information, and purpose
  - Acceptable uses of the technology
  - Acceptable network locations for the technologies
  - List of company-approved products
  - Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
  - Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use

- If vendors, resellers/integrators, or customers can access your payment applications remotely, the remote access must be implemented securely
- Deactivate remote access immediately after use
- Use firewall software on computers connected by a VPN

Examples of remote access security features include:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer)
- Allow connections only from specific (known) IP addresses
- Use strong authentication and complex passwords for logins. Refer to PCI DSS requirements 8.1, 8.3, and 8.5.8–8.5.15
- Enable encrypted data transmission according to PCI DSS requirement 4.1
- Enable account lockout after a certain number of failed login attempts according to PCI DSS requirement 8.5.13
- Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed
- Enable logging functions
- Restrict access to customer passwords to authorized reseller/integrator personnel
- Establish customer passwords according to PCI DSS requirements 8.1, 8.2, 8.4, and 8.5

LogMeIn free or professional client packages meet the data security requirements stated above, as do other remote access technologies, but must be configured for two-factor authentication. For more information, visit LogMeIn at: http://www.LogMeIn.com

Wireless Networks

Chargepath does not require the use of a wireless network and is not supported in a wireless network environment. If you use a wireless network for other purposes in your restaurant, you must take the following precautions to remain PCI compliant.

- If the wireless network is not used by your payment processing systems, make sure that a firewall prevents access to the payment processing systems. **Wireless networks intended for access by restaurant patrons must be completely separated from your computers that process credit card transactions.**

- Wireless networks attached to your payment processing network MUST meet the following PCI DSS requirements:
  - As of April 1, 2009, all newly deployed wireless networks must be using WPA or WPA2 encryption.

  - Existing wireless setups must use WPA or WPA2 encryption when it's an available option. Some older wireless equipment lacks WPA support and this equipment must not be used. It is possible that older wireless hardware can be made compliant with a firmware upgrade that supports WPA or WPA2 encryption. Check with the hardware manufacturer for more information.
  - The default WPA/WPA2 encryption key must be changed to a unique strong key.
  - The default password for accessing the Wireless Access Point's settings must be changed to a unique strong password.
  - Change default SNMP (Smart Network Management Protocol) community strings on Wireless Access Points if SNMP is supported or disable SNMP altogether.
  - Wireless network segments intended to provide public WIFI access must be offered through a wireless access point that is completely separated from your business network segment and your POS network segment by a router firewall that supports Stateful Packet Inspection (SPI) firewall features. This wireless network environment must not allow access to networked devices that store, process or transmit cardholder data.

- Wireless networks attached to your payment processing network are HIGHLY RECOMMENDED to enable additional security:
  - Use wireless keys of 13 random characters containing letters, numbers, and symbols. Keys comprised of words or names are quickly found by criminals using readily available, easy to use tools.
  - Disable SSID Broadcast to make your wireless network less visible to unauthorized users.
  - Use MAC address filtering so that only authorized computers are allowed access to the wireless network.
  - When configuring WPA or WPA2, use the AES option. Only use TKIP when AES is not an available option. Although not severe, there are known weaknesses in TKIP.

More information on network segmentation can be found in the Network Basics and Segmentation section. Recommended network configuration diagrams are available in Appendix A, Recommended Network Configurations. For a more thorough explanation regarding setting up wireless networks, review the PCI DSS Wireless Guidelines document listed on the PCI Security Council's website: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

Network Basics and Segmentation

Switches are network devices that allow you to connect together multiple computers, routers, and wireless access points, firewalls, etc. Switches have multiple network ports, one for each item connected using a network cable. All devices connected to the same switch can communicate with each other without limitation.

Firewalls are network devices that allow you to protect a network segment on the LAN side from the network segment on the WAN side. There are inexpensive ($40-$100) small routers containing firewall functionality that can be found at any store offering computer equipment. These inexpensive routers will work sufficiently so long as they support Stateful Packet Inspection (SPI). Many routers used in restaurant installations feature only a NAT (Network Address Translation) firewall. Be sure yours has an SPI firewall. The router's user manual and the manufacturer's web site are good resources for this information.

Network segmentation is a strategy intended to simplify PCI compliance of your network and to help you protect your business from hackers. At the most basic level, there are three zones representing three levels of risk.

Untrusted Environment – Network connections that anonymous people have access to are considered "untrusted." They should have no network access to your business computers and POS equipment. Business computers should never be connected directly to this zone. Common untrusted networks are the Internet connection itself, customer wireless internet access, and visitor network connections. This is the highest risk zone because anybody can connect to it anonymously. Systems connected to this zone are commonly hacked or get infected with malware and viruses.

Non Card Data Business Environment – Systems not used for payment processing, but are still business-owned fit into this segment. These are systems that can be used for email, web browsing, and other higher risk activity that you would not want to perform on your payment processing systems. On occasion, these systems may become infected with malware and viruses. Once a computer in this zone is infected, the hacker or infection can spread to other systems if they're not protected by a firewall. Note that if any systems in this zone handle credit card data, that data is being put at risk. This is a medium risk zone due to risk of occasional infection. By segmenting these systems into their own zone, the breach is contained. The hacker, malware, or virus doesn't reach your firewall-protected payment processing zone.

Card Data Business Environment – Systems used for payment processing fit into this segment. These systems should only be used for POS activity and should not be used for any other reason. Should these computers become infected with malware or viruses, sophisticated hacking tools can potentially steal sensitive data such as credit cards. The cost of a breach of this zone can be extremely expensive, averaging in the tens of thousands of dollars for a small merchant. This is a low risk zone because it's protected from the other two zones and high risk activities such as web browsing and email do not occur inside it. The chance that hackers, malware, or viruses spread to these systems is minimal.

In summary, to segment your network for security you should:

1) Protect both business environments from the untrusted environment
2) Protect your card data business environment from the non card business environment

For simple network diagrams to help guide your network configuration, see Appendix A, Recommended Network Configurations.

User Management

Administrative access and cashier access to Chargepath is controlled by user accounts. Following are password control requirements for these accounts:

- Default administrative accounts are not available in Chargepath. Each user must have a separate account login.
- All users must have a unique ID
- Group, shared, or generic accounts and passwords must not be used
- Passwords must be changed at least every 90 days
- Passwords must be at least seven characters long
- Passwords must contain both numeric and alphabetic characters
- Passwords must not repeat any of the last four used
- Accounts must lock out after no more than six failed attempts
- Accounts must remain locked out for at least 30 minutes or until an administrator re-enables the ID
- Account logins must time-out and require password re-entry after no more than 15 minutes
- If these procedures are not followed the software will not be compliant with PCI DSS

Windows computers on which the software is used should be protected with user accounts that do not permit software to be installed or system settings to be changed. All measures available to users of Chargepath to prevent access to the Windows operating system should be taken, including preventing users from exiting application software. Administrator accounts used to access the Internet or install Windows updates must be protected with a secure password.

Logging

Administrative access to Chargepath settings is always logged. The software logs the following event information:

- Deletion of users
- Addition of a new user
- Change in user Login Name
- Change in user Full Name
- Change in user Type
- Change in user Password
- Administrator clears a lock on a Cashier's account
- Administrator views logs
- Chargepath Setting change: PCCharge port
- Chargepath Setting change: Temporary test server URL use
- Chargepath Setting change: Require last four digits
- Chargepath Setting change: Default Card Present
- Chargepath Setting change: Allow Address Verification
- Chargepath Setting change: Allow Tips
- Chargepath Setting change: All Merchant Numbers
- Chargepath Setting change: Start with Windows
- Cashier was logged in
- Cashier was logged out
- Cashier password has expired
- New data file was created
- Cashier login attempt failed
- After 6 failed Cashier login attempts a log entry is added; cashier account is locked for 30 minutes
- Administrator was allowed access to the Chargepath Settings window
- Administrator password has expired
- Administrator login attempt failed
- Administrator login to settings/logs was allowed
- After 6 failed Administrator login attempts a log entry is added; cashier account is locked for 30 minutes
- Chargepath program startup
- Chargepath program shutdown (normal shutdown only – absence of this log entry means that the software terminated abnormally)

Logged activity includes the following details:

- Identity of the user who made the changes
- Type of event is identified
- Date and time of event is listed
- Failed events are identified as such
- All administrator activities logged originate in the Chargepath server software
- All cashier activities logged originate in the Chargepath client software

No access is provided in the system for modifying logged administrator activity. Logging is required for the software to be compliant with PCI-DSS. Chargepath logging cannot be disabled.

Virus/Malware Protection and Firewall Software

Every computer on your network must be protected against viruses, worms and malware. Commercially available software intended for this purpose with a current definition database meets this requirement. We recommend *Microsoft Security Essentials* for this purpose. This is free software from Microsoft.

Windows XP, Windows Vista and Windows 7 all have firewall software built-in. Confirm that this feature is activated on every computer on your network. Commercial Internet security software designed for virus and malware protection usually has firewall features than can be used instead of the Windows Firewall. The only exceptions required in firewall software are for the *Chargepath Server* and *Chargepath Client* applications

Chargepath never requires security software to be disabled and security software should never be disabled for any reason.

Using Chargepath with PCCharge Payment Server

You must use version 5.9.1 or above of PCCharge Payment Server with Chargepath to have a PCI compliant system. ***Part of your compliance includes using PCCharge according to the software's Implementation Guide. See your PCCharge documentation for this information.***

Previous Versions of Credit Card Processing Software and Data

If you are converting to Chargepath from either the *Point of Success Mercury Payment Systems Server* or *Point of Success PCCharge Connector*, several steps, some automatic and some manual, are necessary for you to be PCI compliant.

- Prior Point of Success software stored an encrypted credit card number (PAN, or Primary Account Number) in its database for a period of time. After 10 days the encrypted credit card number was automatically removed from each payment record. As a safeguard, the encrypted credit card number field will be automatically removed from the Point of Success database upon installation of the new Chargepath software. Removing the database field eliminates the storage location for the encrypted credit card number and any encrypted PAN stored there. **No user intervention is required for this procedure.**
- Database backups – Point of Success performs automatic, scheduled database backups and also backs up data automatically before a database conversion when a new version is installed. **These database backups contain encrypted credit card numbers and must be manually removed from your computer after installing Chargepath.** Follow these instructions on the server (data host) computer:
  - Go to Start > My Computer > Local Disk C: > Point of Success > Backup. In this folder you will find the pre-conversion data backup files. Each complete backup set is stored in one file with a .dbz file name extension. These backup files must be copied to removable media, preferably an optical disc because it is easier to destroy when these data backups are no longer needed, and deleted from the server.
  - Go to Start > Local Disk C: > Point of Success > Backup > POS Data. This folder contains backup files created by the scheduled backup feature in Point of Success. Each complete backup is stored in one file with a .dbz extension. These backup files must be copied to removable media, preferably an optical disc because it is easier to destroy when these data backups are no longer needed, and deleted from the server.
  - Credit card processing program files in previous versions of Point of Success contain a static cryptographic key used to encrypt the credit card number. These files will be removed automatically when Chargepath is installed. **No user intervention is required for this procedure**.
  - **Secure deletion of files is required.** The easiest method is to securely delete the contents of the Windows Recycle Bin and securely clean hard disk free space after deleting Point of Success backup data files. We recommend **Eraser**, a free secure deletion utility. This software is available on the Internet at http://www.sourceforge.net/projects/eraser. Complete help documentation is included with the software explaining how to securely delete the contents of the Windows Recycle Bin and clean unused hard disk space. See the "Securely Deleting Files with Eraser" section of the Implementation Guide for instructions on using Eraser to delete your sensitive data.
- Prior Point of Success software never stored magnetic stripe data, card validation codes, PINs or PIN blocks. Because this data was not stored, **no user intervention is required to remove this data.**

Securely Deleting Files with Eraser

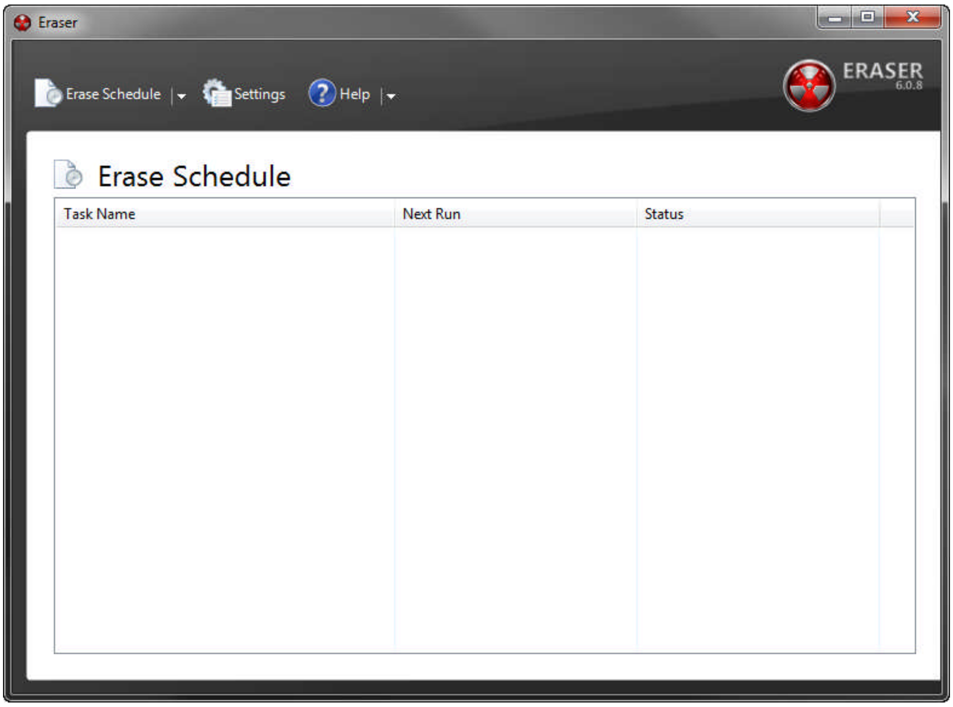
Note: The following instructions for using *Eraser* to securely delete sensitive credit card data are provided as a convenience. Inborne Technology Corporation assumes no responsibility for your use or inability to use these instructions or for the correct operation of the Eraser software. Eraser software is provided by an independent software developer who would appreciate your support of this Open Source software project.

These processes are hard disk intensive and may take a substantial amount of time to complete, depending on the size and performance of your hard disk drive. Allow plenty of time to finish before you need to use the computer!

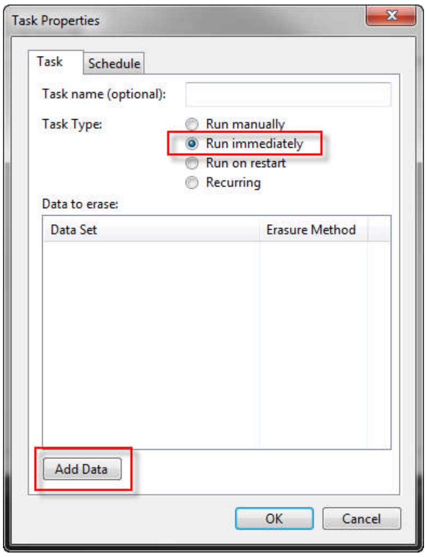
The following instructions are based on "Eraser" version 6.0.8. Using Eraser to securely delete past credit card data needs to be done only once after these steps are completed:

- Install Chargepath
- Make a backup copy of your database backups onto removable media

Install and launch Eraser. The main menu will appear:



Right-click in the *Erase Schedule* list area and select *New Task*. This window will display:



Task Properties

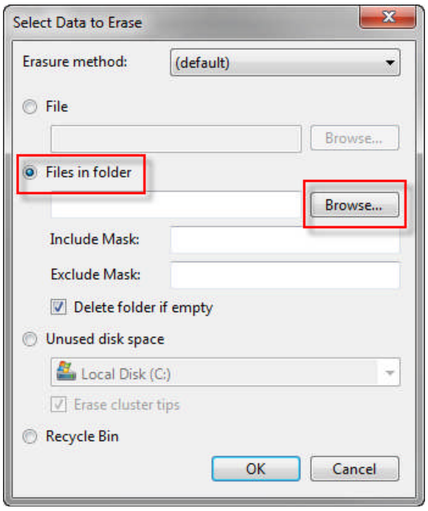
Task name (optional):

Task Type:
○ Run manually
● Run immediately
○ Run on restart
○ Recurring

Data to erase:

Data Set	Erasure Method

Select Run Immediately and click the Add Data button to choose the files to erase:



Select Data to Erase

Erasure method: (default)

○ File

● Files in folder

Include Mask:

Exclude Mask:

☑ Delete folder if empty

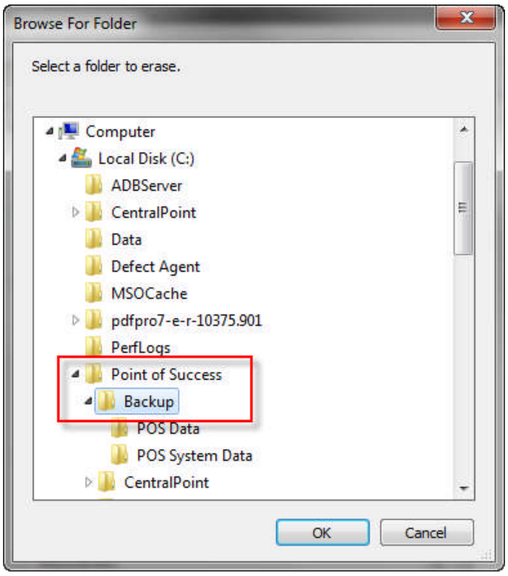
○ Unused disk space

Local Disk (C:)

☑ Erase cluster tips

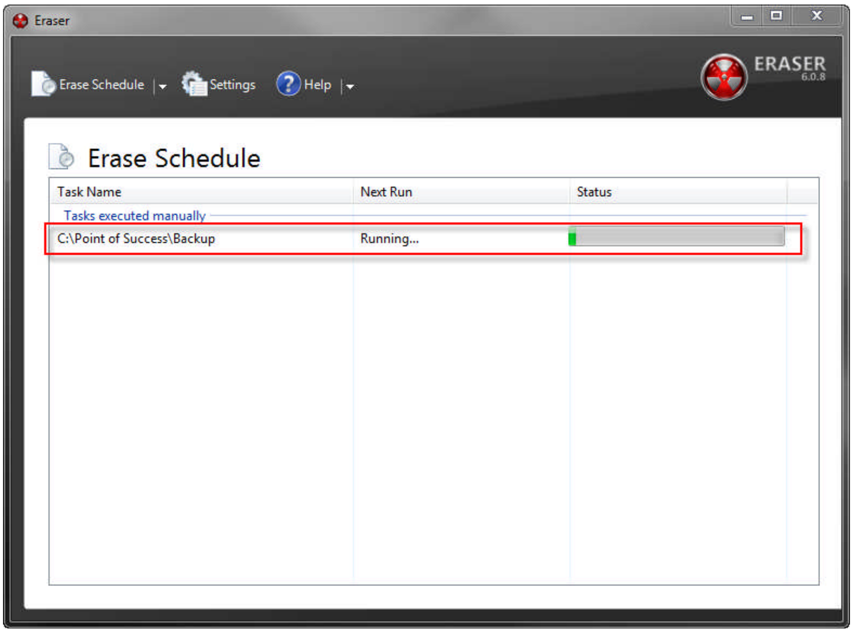
○ Recycle Bin

Click to select *Files in Folder*, then click the Browse button to select the folder:



Select a folder to erase.

Browse to My Computer > Local Disk C: > Point of Success and select the *Backup* folder. Click OK to close the Browse window, then click OK to close the Task Properties window. The secure delete operation for all the files in the Backup folder will begin immediately.



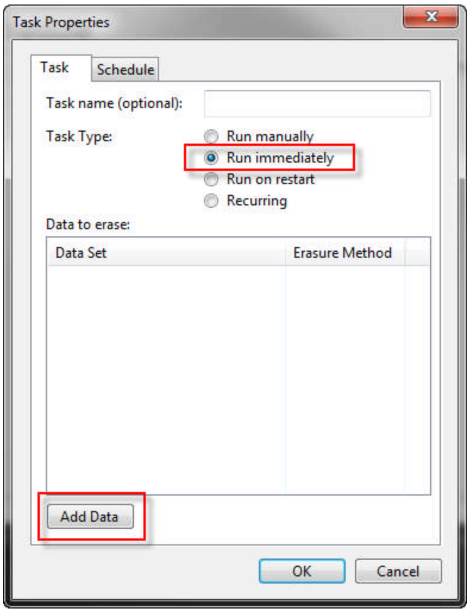
Erase Schedule

Task Name	Next Run	Status
Tasks executed manually		
C:\Point of Success\Backup	Running...	

Upon successful completion, all the data backup files on the server’s hard disk drive will be securely deleted.

Next, securely delete unused disk space using these instructions:

Right-click in the *Erase Schedule* list and select *New Task*. The following window will display:



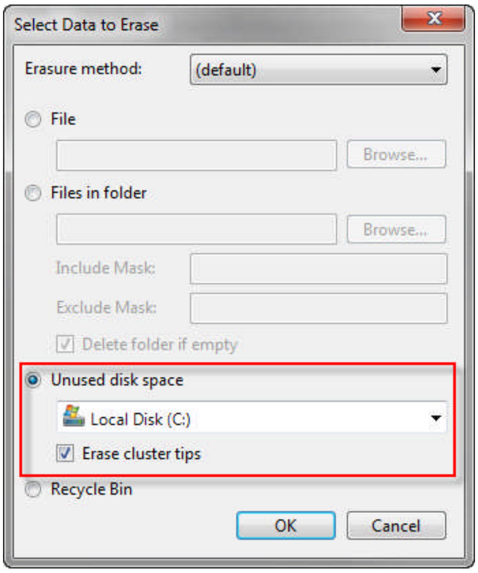
Task name (optional):

Task Type:
○ Run manually
● Run immediately
○ Run on restart
○ Recurring

Data to erase:

Data Set	Erasure Method

Select *Run Immediately* and click the *Add Data* button. This window will display:



Erasure method: (default)

○ File

○ Files in folder

Include Mask:

Exclude Mask:

☑ Delete folder if empty

● Unused disk space

Local Disk (C:)

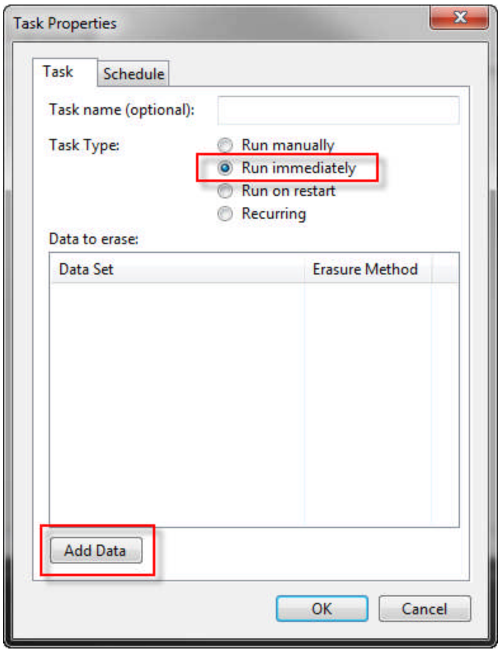
☑ Erase cluster tips

○ Recycle Bin

Select *Local Disk C:* and click OK. Click OK in the *Task Properties* window and the secure delete operation will begin immediately. Upon completion, all unused space on the hard disk will be securely overwritten.

Finally, securely delete the contents of the Recycle Bin.

Right-click in the *Erase Schedule* list and select *New Task*. The following window will display:



Task Properties

Task | Schedule

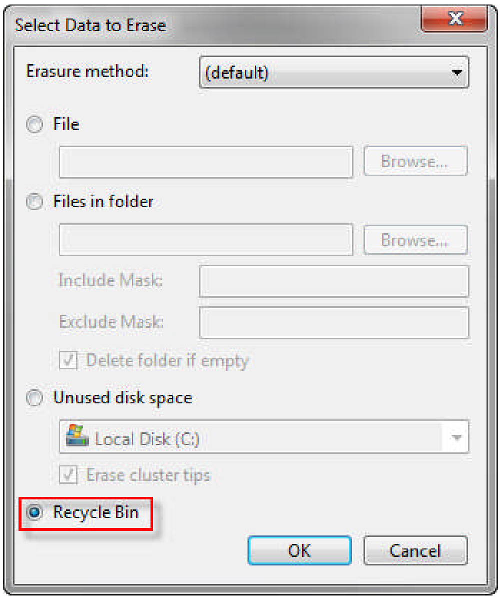
Task name (optional):

Task Type:
○ Run manually
● Run immediately
○ Run on restart
○ Recurring

Data to erase:

Data Set	Erasure Method

Select *Run Immediately* and click the *Add Data* button. This window will display:



Select Data to Erase

Erasure method: (default)

○ File

○ Files in folder

Include Mask:

Exclude Mask:

☑ Delete folder if empty

○ Unused disk space

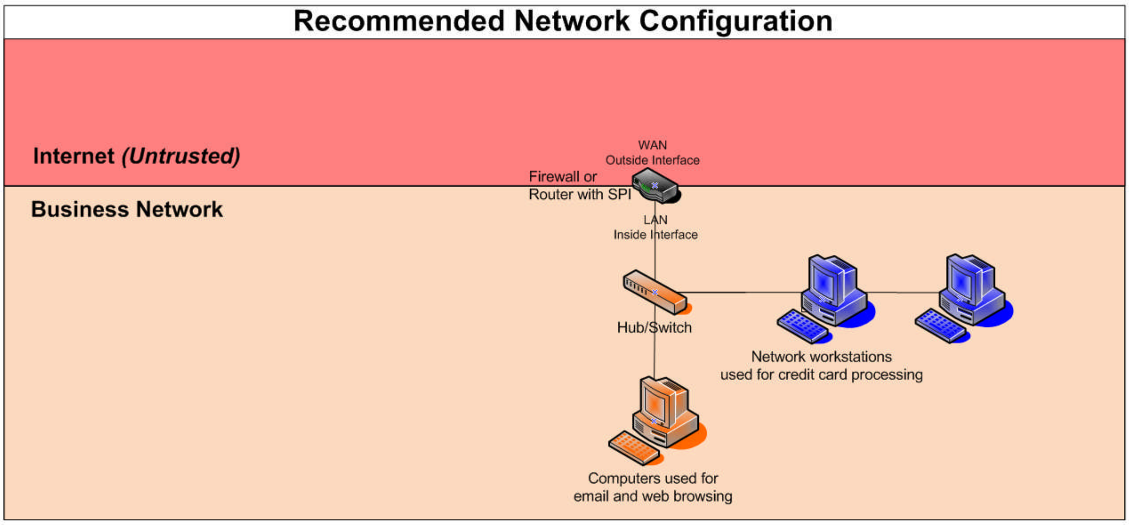
Local Disk (C:)

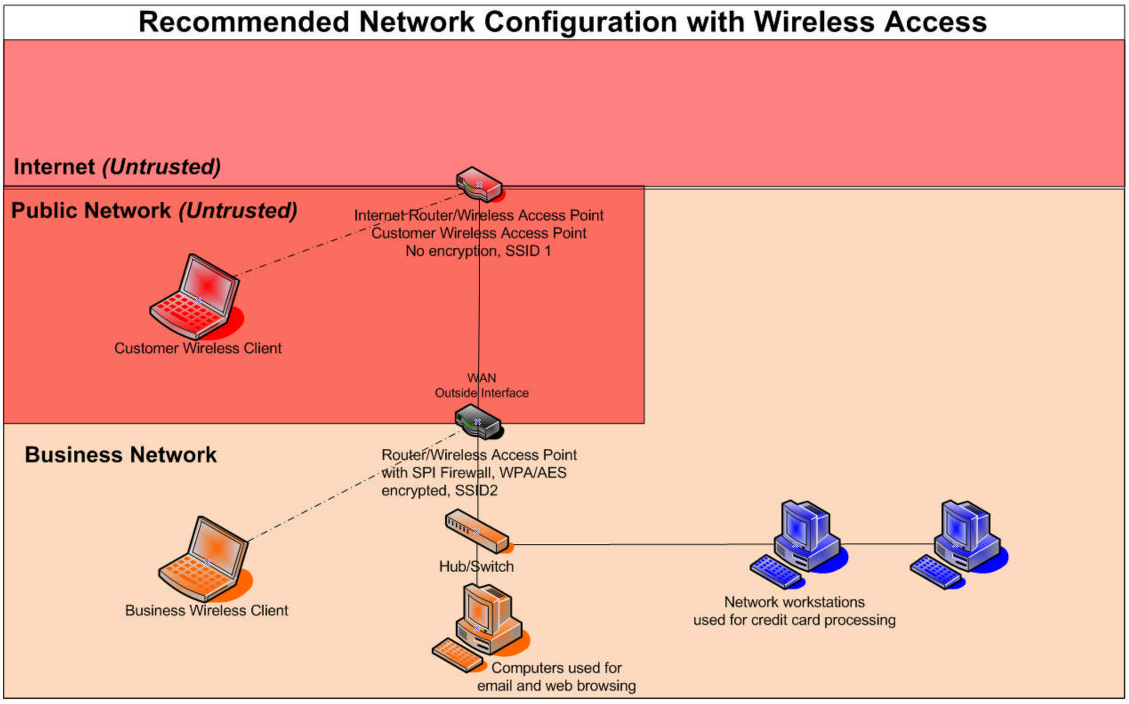
☑ Erase cluster tips

● Recycle Bin

Click to select *Recycle Bin*, then click OK. Click OK in the *Task Properties* window and the secure delete operation will begin. Upon completion, the contents of the Recycle Bin will be securely deleted.

Appendix A:
Recommended Network Configurations




Recommended Network Configuration with Wireless Access
Internet *(Untrusted)*
Public Network *(Untrusted)*
Internet Router/Wireless Access Point
Customer Wireless Access Point
No encryption, SSID 1
Customer Wireless Client
WAN
Outside Interface
Business Network
Router/Wireless Access Point
with SPI Firewall, WPA/AES
encrypted, SSID2
Hub/Switch
Business Wireless Client
Network workstations
used for credit card processing
Computers used for
email and web browsing