AutoClerk Inc.'s
Payment Card Industry (PCI)
Payment Application Data Security Standard (PA-DSS 2.0)
Implementation Guide
For AutoClerk Version 9
January 2014

Table of Contents

AutoClerk, Inc.

Address: 936 Dewing Ave., Suite G, Lafayette, CA 94549

Phone: 925.284.1005

Fax: 925.284.3423

URL: www.autoclerk.com

Version	Date	Reviewed by	Changes made
2.1	10/14/13	Ed Bear	First pass at document for PA-DSS
2.2	10/22/13	Holly McGlothlin	Reviewed Ed's document, cleaned up typos, grammar, citations, formatting
2.3	10/24/13	Ed Bear	Reviewed Holly's changes
2.4	1/31/14	Holly McGlothlin	Added Version Table, updated date

Introduction

AutoClerk, Inc. is a software application developer and vendor. As a vendor that integrates and implements credit card processing for deposits, authorizations and payments, we are required to comply with the *Payment Card Industry's (PCI) Payment Application Data Security Standard (PA-DSS)*.

As a business entity that processes credit cards, in terms of both getting authorizations as well as processing sales, you are required to be compliant with *the Payment Card Industry Data Security Standard (PCI DSS)*. There are several levels of PCI DSS compliance. One criterion is the number of credit card transactions processed in a year. You need to review the compliance documentation at http://www.pcisecuritystandards.org and take the necessary steps to obtain and maintain your appropriate PCI DSS compliant status.

AutoClerk, Inc.'s PA-DSS compliance serves to support your PCI DSS compliance. Our being PA-DSS compliant does *not* make you PCI DSS compliant.

The PCI DSS consists of 12 Requirements, which cover the handling, processing and storage of credit card data. The following table lists the requirements.

Objective	**12 PCI-DSS Compliant Requirements**
Build and Maintain a Secure Network	Requirement 1: Install and maintain a firewall configuration to protect cardholder data Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Requirement 3: Protect stored cardholder data Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	Requirement 5: Use and regularly update anti-virus software or programs Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Requirement 7: Restrict access to cardholder data by business need to know Requirement 8: Assign a unique ID to each person with computer access Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks	Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses information security for employees and contractors.

This PA-DSS Implementation Guide explains AutoClerk's -role in the security of your guests' credit card data. It instructs you and your network administrator how to enable security settings in regards to both your network and hardware. It instructs you on secure AutoClerk product implementation; and defines some of your responsibilities for meeting PCI DSS requirements.

Following these guidelines does *not* make you PCI DSS compliant, nor does it guarantee your network's security. It is your responsibility, along with your network administrator, to ensure that your hardware and network systems are secure from internal as well as external intrusions.

AutoClerk makes neither claim on the security of your network, nor on the level of your PCI DSS compliance.

AutoClerk Version 9 can only be updated from AutoClerk Version 8, which does not allow the storing of legacy data even from previous versions of AutoClerk. (PA-DSS 1.1.4.a)

Anytime AutoClerk was installed at your property, you were required to follow AutoClerk's System Specifications (Specs). You must review the current Specs and have your network administrator verify that your AutoClerk system meets them. There may be changes which need to be made to bring your system to AutoClerk's current specs. Following AutoClerk's Specs does *not* make you PCI DSS compliant; however, it contributes to your PCI DSS compliance. AutoClerk's System Specifications can be found at http://myautoclerk.com. Once you have logged in, there is a link on the home page. AutoClerk's Specifications are also attached as "Appendix B" to this document.

This document is organized by the PA-DSS requirements, which AutoClerk must meet to be PA-DSS certified. Some of the measures you need to take are detailed in the AutoClerk System Specifications. This Guide also references the PCI DSS (Version 2.0 October 2010) and the attached Appendixes.

1. Do Not Retain Full Magnetic Stripe, Card Verification Code or Value (CAV2, CID, CVC2, CVV2) or PIN Block Data

The magnetic stripe on the back of a credit card contains sensitive data including the cardholder's name, Primary Account Number (PAN), expiration date, and other information necessary to process the card for an authorization and/or sale. The Card Validation Code or Value, or Card Security Code refers to either 1) the data element on a card's magnetic stripe or 2) the 3-digit number next to the signature field on the back of a Discover, JCB, MasterCard, and Visa payment card; or the 4-digit number on the face of an American Express card. A PIN (Personal Identification Number) is used when a debit card is processed as a debit transaction rather than a credit card transaction.

AutoClerk's credit card interface (Data capture) is certified with Shift4 and Heartland Payment Systems. Shift4 and its "Dollars on the Net™" is "a real-time payment gateway between merchants' point-of-sale systems and their bank/processor". By processing guests' credit cards through Shift4 or Heartland Payment Systems, the credit card number is kept by the AutoClerk PMS on your hardware as a masked number with a token. A token is a unique code, which represents and points to the actual card number, which resides at Shift4 or Heartland Payment Systems

"Masked" is when a cardholder's PAN has been substantially replaced by X's. For example, XXXXXXXXXXXX4957 is a masked format used when viewing and/or printing a guest folio receipt in AutoClerk; 5474XXXXXXXX4957 is a masked format used by Shift4, Heartland Payment Systems, and/or AutoClerk for a hotel's internal reporting purposes, such as a Transaction report.

AutoClerk requires *all* properties which have the AutoClerk data capture interface use Heartland Payment Systems or Shift4 as the property's payment gateway.

When a credit card is used within the AutoClerk client for an authorization or sale it is either swiped through a magnetic card reader or the card data manually entered. The data is then sent by the AutoClerk client to Shift4's Universal Transaction Gateway (UTG) or to Heartland Payment Systems. Shift4 and Heartland Payment Systems process the card authorization and/or sale and return the number in encrypted format to AutoClerk as a truncated number and a token. The full magnetic stripe data is not kept on your hardware and the tokens that are returned by Shift4 Heartland Payment Systems are of no value to a thief.

When a credit card number is manually entered into the PMS for an authorization and/or sale, the staff has the ability to include the name on the card, the card's validation code or value as well as the billing address's zip code. If the card's code and/or value is entered, neither are retained anywhere within the AutoClerk PMS. They are passed to Shift4 or Heartland Payment Systems who uses them only to further validate the card. They are not returned to the PMS once an authorization or sale is obtained.

A debit card's PIN and/or PIN block data is one of the most dangerous numbers to retain. The AutoClerk PMS does not support pin-based debit transactions. AutoClerk's

credit card interface does not allow for the processing of debit cards as anything other than a credit card; therefore, transmitting the PIN is not possible.

When a reservation is entered in the PMS, a property typically requires a valid credit card number and expiration date to guarantee it. Once the credit card number is entered, it is sent to the AutoClerk PMS' which encrypts the card information. Anyone looking at the reservation sees a masked credit card number and expiration date. AutoClerk's reservation form does not have a field to enter the Card Validation Code/Value and/or the PIN block data, so any card validation codes/values and PIN block data are also not kept within the PMS.

AutoClerk masks PANs and expiration dates on reports and also encrypts them on backups. The PMS' backups are compressed using zip and are kept on the AutoClerk server computer, on zip disks, on other removable media, and/or sent off site.

AutoClerk Version 9 can only be updated from AutoClerk Version 8, which does not allow the storing of legacy data even from previous versions of AutoClerk. (PA-DSS 1.1.4.a)

There may be instances when you need to retrieve a guest's full credit card number and expiration date. Depending on the situation, you will get the card number and expiration date from either Shift4's Dollars on the Net™ website, a phone call to Heartland Payment Systems or from within the AutoClerk PMS.

The AutoClerk PMS can show an unencrypted credit card number only on an existing reservation and only to specific staff. View ability is based on user permissions which are set by property management through the PMS' ACAdmin program. All views of unencrypted credit cards numbers held in the PMS are logged by AutoClerk. You must limit the number of staff who has access to this data. When setting up your users in AutoClerk, only those employees on a "need to know" basis should have access to read full card numbers, process refunds, etc. (PCI DSS Reqs. 7.1, 9).

AutoClerk retains active reservations that do not have an advance deposit posted to them for 60 days past the arrival date. These reservations have a status of guaranteed, hold, share-with, wait list, checked in/out, no show, or canceled. During that time, an authorized staff member has the ability to go back and retrieve a guest's unmasked credit card information. If a reservation has an advance deposit posted to it and it is not checked in, it will remain in the reservation file until the Deposit balance is $0.00, and then will be purged based on its arrival date. The ability to see an unmasked credit card in a past reservation also depends on your property's retention period as discussed in Section 2 of this document.

Per PA-DSS 1.1.5.c, AutoClerk support staff, customers and integrators will: collect sensitive authentication only when needed to solve a specific problem; store such data only in specific, known locations with limited access; collect only the limited amount of data needed to solve a specific problem; encrypt sensitive authentication data while stored; and securely delete such data immediately after use.

2. Protect Stored Cardholder Data

PA-DSS 2.1 requires the following guidance for customers and integrators: That cardholder data exceeding the customer-defined retention period must be purged. We must provide a list of all locations where the payment application stores cardholder data (so that customers know the locations of data that needs to be deleted). Finally, we must provide instructions for configuring the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture of retention of cardholder data. For example, system backup or restore points.

Protecting cardholder data includes the following: 1) Purging cardholder data after a customer-defined retention period, 2) Masking and truncating card numbers, 3) Protecting cryptographic keys, and 4) Securely deleting any cryptographic keys in previous versions of AutoClerk.

There is a setting in AutoClerk that allows a property to define 1) How often AutoClerk checks and 2) A retention period, after which, AutoClerk purges cardholder data. Both parameters are expressed in days. Purging of cardholder data beyond a customer defined retention period is required per PCI DSS.

AutoClerk stores credit card data in four files: Reservations, Group masters, Inhouse folios, and Folio history. When AutoClerk checks these files at the defined interval, cardholder data is selected for purging according to the following criteria:

1. All Reservations except Permanent Reservations: Departure date is older than today - <retentionperiod>.
2. Permanent Reservations: Reservation creation date is older than today - <retentionperiod>.
3. Group Masters: The later of (group departure date, last room block) is older than today - <retentionperiod>.
4. Inhouse folios: (1) Folio is checked out, and departure is older than today -2, or (2) Folio is checked in, and arrival is older than today - <retentionperiod>.
5. Folio History: Departure date is older than today - <retentionperiod>.

The credit card data is cleared by encrypting the truncated credit card number over the encrypted full card number and rewriting the record. A manager can also run the utility at any time to purge cardholder data past a defined number of days.

What does this mean to the hotelier? For example, let's assume a hotel manager defines a check interval of 7 days and retention period of 90 days. Then AutoClerk will, automatically, every 7 days, on the night audit, examine the cardholder data locations and clear sensitive cardholder data per the rules stated above.

Prior to purging, a user with view rights can see a full credit card number on a reservation. Post purging, even with view rights, all the user will see is a truncated and masked credit card number on a reservation. Credit card data which is part of an advance deposit folio, inhouse folio credit card data, and historical folio history already is truncated and contains a token from Shift4 or Heartland Payment Systems.

The nalog.txt, which is produced at each night audit, logs the purging which took place during that audit.

AutoClerk's PMS responsibility is to make sure that any PAN is masked when displayed, but can be displayed "to those employees and other parties with a specific need to see full PAN". The PAN is unreadable anywhere it is stored. The PMS stores credit card PANs using encryption or tokenization. The full credit card data is stored at Shift4 or Heartland Payment Systems. The reports and historical data produced and maintained by the PMS contain only the truncated credit card numbers and expiration dates.

AutoClerk uses two (2) cryptographic keys: a Key-Encryption-Key (KEK) and a Data-Encryption-Key (DEK). The KEK is used to encrypt/decrypt the DEK; the DEK is used to encrypt/decrypt the data. Both keys are stored in the server registry in binary format. They are protected by the Windows registry protection mechanism which, when properly set up, prevents access by any network user or any user of the same computer without the correct credentials. The KEK is also protected by being obfuscated using an internal encryption routine. You are strongly advised to restrict access to keys to the fewest number of custodians necessary and store keys securely in the fewest possible locations and forms. (PA-DSS Req. 2.5.c)

The keys have expiry dates. The Encryption Key Expiration report is produced by the night audit. It lists the keys' expiration date. The report can also be produced at will through the Utilities menu.

When the credit card encryption keys have expired, or on demand, an AutoClerk administrative user can invoke a program through ACAdmin that generates two (2) new keys, re-encrypts every cc number in the data set using the new DEK, and stores the new keys.

Properties can change the encryption keys at any time. They must change them when it they expire, anytime they suspect their data has been comprised, or when the integrity of the keys have been weakened. (PA-DSS 2.6.5)

AutoClerk does not retain retired or replaced cryptographic keys making them irretrievable. (PA-DSS Reqs. 2.6.5.c, 2.7.a) Irretrievability is absolutely necessary for PCI DSS compliance.

AutoClerk's backups are encrypted using two (2) keys. The backup encryption keys must be entered and kept by two separate employees. When the backup keys are changed, each key custodian enters their key manually, and stores it per the property's security policy. When the keys are entered, they are not clear-text.

"Appendix C" in this document contains a sample Key Custodian form (PA-DSS Req. 2.6.a and PCI DSS Req. 3.6) which all key custodians should complete and keep in a secure place.

The only cryptographic key material in earlier versions of the AutoClerk client was a built-in credit card encryption key in executables such as ac2g.exe and bw.exe. Part of the AutoClerk conversion/upgrade process to Version 8 includes securely deleting all instances of the AutoClerk PMS client executables within the active data. This process securely deletes any cryptographic key material and/or cryptogram from previous versions in the active data and makes them irretrievable.

3. Provide Secure Authentication Features

Per AutoClerk's System Specifications (“Appendix B”), and a requirement for your PCI DSS compliance, every employee who has computer access must have a unique user name and password on every computer they use. (PCI DSS Reqs. 8.1, 8.2, 8.5.8 through 8.5.15)

Every employee using AutoClerk must have a unique user name and password that is used when they log into an AutoClerk session. You cannot have duplicate user names or initials. AutoClerk passwords must be at least 7 characters and contain at least one number and one letter. In addition, they can contain upper and lower case letters, and/or special characters (e.g., punctuation). Setting up a user's login name and password must be done immediately upon their hire. Do *not* set up or use any default AutoClerk user accounts or passwords. A manager must have two user accounts in AutoClerk: one for everyday use and another to administer user names and passwords within AutoClerk's ACAdmin program.

AutoClerk enforces secure changes to authentication credentials by the completion of installation by providing a user name with a one-time use password. This allows the manager to access ACAdmin to then set up all the AutoClerk users. Customers and integrators are advised to assign secure authentication to any default accounts (even if they won’t be used), and then disable or do not use the accounts. (PA-DSS 3.1.a)

AutoClerk's users' passwords expire after 90 days and then must be reset. The new password cannot be any of the past four passwords. If an AutoClerk PMS user fails to log into a terminal 6 times, they will be locked out of that terminal for 30 minutes. Rebooting the terminal does not shorten the timeout of this feature. Your network vendor must set up all computers to require Windows logon if the station has been idle for more than 15 minutes. All AutoClerk PMS user passwords are encrypted and are never seen in clear-text. In addition, all login attempts are logged by the PMS server and are viewable through ACAdmin.

When an employee leaves your employment, you must immediately delete *all* their users’ logins in Windows, in the PMS, and in Shift4 or Heartland Payment Systems. Take any other steps necessary depending upon the duties and/or access the ex-employee had, such as changing locks on storage areas for credit card data or being a key custodian.

AutoClerk strongly advises its customers and integrators to control access, via unique user ID and PCI DSS compliant secure authentication, to *all* systems, PCs, servers, and databases that contain payment applications and/or cardholder data. (PA-DSS 3.2)

Your property's written security policy must include your rules regarding users, passwords and access to ALL credit card data whether it is on the active dataset, within Shift4 or Heartland Payment Systems, on removable backup media, and/or on paper.

4. Log Payment Application Activity

The AutoClerk PMS automatically creates a variety of logs, such as credit card logs and user access. (PA-DSS 4.1) Credit card logs include the logged in user identification (clerk ID), type of event (I.e. Authorization), date and time, success or failure indication (I.e. Approved), origination of event (Shift and Station Number), Identify or name of affected data, system component, or resource (Room/Folio Code).

AutoClerk's PMS server application logs those events that affect security including each time a staff member logs into AutoClerk, successful or not, when an employee views an unmasked credit card PAN and expiration date; as well as actions taken by an AutoClerk PMS administrator. These logs are accessible to an AutoClerk administrator logged into AutoClerk's ACAdmin module.

Logs are automatically created; they cannot be configured or disabled by the user. (PA-DSS 4.1.b) Logs are automatically exported into a CSV or text file. The log files are located on the property's server computer in:
\app\autoclerk\060.002\hotelid\logs
\autoclerk\hotelid\data\credit

These logs can be imported into any standard centralized logging system. To access the logs, you must log onto the AutoClerk server computer as an administrator. From the centralized logging system, you must Import the data. The file type should be CSV or text. (PA-DSS 4.4.b)

5. Develop Secure Payment Applications

This section of the *PA-DSS Requirements* applies to AutoClerk, Inc. and how we write, develop, test, and implement our software application. It is important you are made aware of how the PMS is developed, tested, released, and implemented to aide you in complying with PCI DSS.

Prior to being released to our clients as either a beta or a production version, all upgrades to the AutoClerk PMS and interface applications are tested in-house under the direction of our QA department per their test plans. If necessary, "test only" credit cards issued by Shift4 and Heartland Payment Systems are used during the test period. No active or "live" credit card numbers are used.

Before a new property is put online with AutoClerk, a dataset is created from an Installation form filled out by the property as part of their online process. No test or individual guest credit card information is used when creating the property's dataset.

Development, testing, and production are separate departments at AutoClerk. Any new code comes from development to QA. QA oversees the testing of the new code. Once satisfied, QA then passes it to Operations for implementation in the field by the Tech department. The code passed from QA to Production to be implemented in the field is an executable file. No test data is included.

When a new version is implemented at a property, the General Manager is advised they can go to http://www.myautoclerk.com for the version release notes. They can also find documentation there on the use of new features.

The following are all required protocols (TCP/IP), services (Pervasive and Shift4's UTG), components and dependent software and hardware (card readers by Magtek) that are necessary for any functionality of the payment application, including those provided by third parties. (PA-DSS 5.4.c)

6. Protect Wireless Transmissions

Wireless connections to the AutoClerk network segment are not recommended.

If *any* workstations are wirelessly connecting to your network, they *must* be configured to use industry best practices such as IEEE 802.11i to implement strong encryption for authentication and transmission. It is prohibited to implement WEP.

In addition, if wireless is used, customers, integrators and/or your network administrator must:

1) Verify all encryption keys are changed from default at the time of installation and are changed if anyone with knowledge of the keys leaves the company or changes positions

2) Change the SNMP community strings

3) Change all default passwords/passphrases on access points

4) Update firmware is updated to support strong encryption for authentication and transmission over wireless networks

5) Verify other security-related wireless vendor defaults are changed

6) Install a firewall between any wireless networks and systems that store cardholder data

7) Configure firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PA-DSS 6.1.f)

Your network administrator must verify that the wireless technology is protected with personal firewall software. The firewall software secure configuration must not be alterable by an employee. All vendor defaults, including keys, are changed at installation and whenever the person knowing the key leaves or changes positions; SSID broadcast is disabled; default Simple Network Management Protocol (SNMP) community strings are changed; all access point passwords are changed; WPA or WPA2 are enabled, if possible. At all times, industry best practices to implement strong encryption for authentication and transmission of cardholder data must be implemented. (PA-DSS 6.2.b)

7. Test Payment Applications to Address Vulnerabilities

This section of the PA-DSS refers to AutoClerk's internal processes, which keep AutoClerk up to date on potential security risks to the AutoClerk program and credit card data.

If any possible threats are found to the AutoClerk application, they are investigated, fixed, tested, and deployed to our customers in a “timely” manner. All updates are delivered securely via two-factor authentication and through our internal “chain-of-trust.”

It is your responsibility to do the same for your network, including having your network administrator run regular network scans to check for any intrusions and/or unauthorized access attempts. Internal and external network vulnerability scans must be run at least quarterly by a PCI approved scanning vendor, as well as after any significant change in your network. In addition, intrusion-detection systems must be installed to monitor all traffic in the cardholder data environment and to alert personnel to any suspected compromises.

8. Facilitate Secure Network Implementation

You must have certain security tools in place. These tools include, but are not limited to, an external hardware firewall, anti-virus software, and traffic filtering devices.

Updates to these entities such as your Windows Operating System, anti-virus program, etc., need to be managed, monitored, and installed. Be sure your network administrator installs these tools and trains management and staff on their use, management, and maintenance.

Having these security tools implemented on your network computers does *not* interfere with the AutoClerk PMS when they are properly configured.

9. Cardholder Data Must Never be Stored on a Server Connected to the Internet

AutoClerk does not use a web server or database server, therefore PA-DSS 9 does not apply. (PA-DSS 9.1.b)

10. Facilitate Secure Remote Access to Payment Application

Two-factor authentication must be used whenever *anyone* accesses your network remotely. Two-factor authentication requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession e.g. smartcards or hardware tokens; and something they know e.g. a password. To access a system, the user must produce both factors. (PA-DSS 10.2)

For all remote access, you *must* use and implement remote access software security features such as requiring a unique user name, authenticating all users, changing all default settings, enabling lockouts, enabling data encryption, enabling logging, allowing connections only from specific (known) IP/MAC addresses, and establishing customer passwords according to the PCI DSS requirements. PCI compliant use of all remote stations must be part of your property's security policy.

AutoClerk does not interfere with outside entities using two-factor authentication to access your network. AutoClerk support staff use two-factor authentication whenever we need to gain access to a hotel's network. All remote access by AutoClerk support is facilitated by known secure hardware solutions by trusted providers such as Bomgar, RSA Labs, etc.

AutoClerk support sessions are facilitated by a security appliance called the “Bomgar Box™.” This appliance is owned, administered, and hosted by AutoClerk. Our appliance is integrated with AutoClerk's Radius server and can only be used by AutoClerk employees with a current, valid RSA token code. This code changes every 60 seconds. Each employee is issued their own RSA security token.

Support sessions to our hotel customers can be conducted in the following ways:

1. Customers can initiate an AutoClerk support session by visiting esupport.autoclerk.com from a browser on the station at which they work and entering a 7-digit pin code our support agent gives them over the phone. That pin is good for that particular support session only.
2. An AutoClerk support agent may email a link to the customer.
3. The link may be accessible via other locations.
4. The client software may be permanently installed on hotel computers, such as dedicated server computers.

Under extraordinary emergency conditions that arise when Bomgar is not working, a non-Bomgar communication will be used per the demand of the hotelier or the hotelier’s network administrator. When such extraordinary conditions arise as a business requirement, the Tier 2 AutoClerk technician will log the following information into our customer support database:

1. Name of hotel
2. Communication method

3. AutoClerk technician's name
4. Date and time
5. Reason for not using Bomgar.

Instructions for Customers and integrators: Regarding secure use of remote-access technologies, specifying that remote-access technologies used by vendors and business partners should be activated only when needed and immediately deactivated after use.

AutoClerk recommends customers and integrators use a securely configured firewall or a personal firewall product if a computer is connected via VPN or other high-speed connection and to secure these "always-on" connections, per PCI DSS Requirement 1 and 12.3.9. (PA-DSS 10.3.1)

AutoClerk requires that the computer running AutoClerk's AutoServe program have high-speed Internet access. It must be persistent and static and must be accessible via public (not private) address. Examples of such broadband services would be: DSL, T1, or Cable Modem. AutoClerk does not access properties via a dial-up modem.

Because the server has a static and persistent IP, it must be secured behind your hardware firewall. Proper configuration of the firewall will allow access only to those approved vendors/persons/entities. Any Regional stations must also have at minimum, a personal software firewall installed and properly configured in a secure manner.

When AutoClerk support staff access your system to install updates to the AutoClerk PMS, we access the property using Bomgar and two-factor authentication. The two-factors are a combination of: 1) An encrypted hardware solution (Bomgar), 2) Unique usernames and passwords, 3) One-time use PIN from a RSA token, and 4) The remote user/customer initiating the connection. The Bomgar solution will not interfere with RADIUS, TACACS, or corporate VPNs. All remote access is logged by Bomgar. These remote technologies should only be activated when needed by business and vendors partners and should be deactivated immediately after use. Customers and resellers/integrators should use a securely configured firewall or personal firewall product if the computer is connected via a VPN or other high speed connection, to secure these "always-on" connections. (PA-DSS 10.3.1 and PCI DSS Requirement 1)

Per PA-DSS 10.3.2.b, if integrators or customers can use remote access software you are instructed to use and implement remote access security features.

11. Encrypt Sensitive Traffic over Public Networks

Customers and integrators are to use strong cryptography and security protocols. (PA-DSS 11.1.b)

AutoClerk has the ability to send guests a reservation, cancellation and/or thank you letters via email. However, even if the letters are formatted to send the guest's credit card number used to guarantee the reservation, it sends the masked PAN and only the last four digits of the number. The full PAN is never sent from the PMS. (PA-DSS 11.2.b)

12. Encrypt All Non-Console Administrative Access

The AutoClerk program does not have non-console administrative access.

We recommend the use of strong cryptography, using technologies such as SSH, VPN, or SSL/TLS (PA-DSS 12.1 and PCI DSS Req. 2.3).

13. Maintain Instructional Documentation & Training Programs for Customers, Resellers, & Integrators

AutoClerk's website for our customers and integrators is http://www.myautoclerk.com. It contains: AutoClerk's System Specifications (for integrators and customers), a link to our interactive training videos, training documentation, and the Release Notes, which we provide for each version and/or update (available under the "Documentation" tab). Customers can also select Help at the top of the PMS Main menu to get access to documentation.

Prior to AutoClerk's installation, a link to this document is provided to the property. It is also given to integrators. The *AutoClerk PA-DSS Implementation Guide* can also be found at http://www.myautoclerk.com.

It is reviewed and updated at minimum on a yearly basis, and is updated as needed to document all major and minor changes to the payment application (AutoClerk) as well as to document changes to PA-DSS requirements. (PA-DSS 13.1.2.a, PA-DSS 13.1.2.b, PA-DSS 13.2)

Appendix A: Legacy Data Secure Deletion Instructions

Security Disclaimer

The AutoClerk Licensee (Customer) acknowledges that no computer system or software can be made completely secure. The information and instructions detailed below do *not* guarantee the safety or security of your hotel's e-commerce network or information transmitted or stored on this application. In addition, following these steps does *not* make the Customer PCI DSS compliant; although, it does support your effort to become compliant. Not completing these steps to delete securely and then wipe all legacy data makes the hotel *non*-PCI DSS compliant.

The secure deletion of AutoClerk PMS legacy data *must* be performed by the hotel's network administrator on *every* hotel computer. The access, retention, storage, and deletion of other forms of legacy data are the property's responsibility and must follow your written policy.

The purpose of performing these steps is to delete securely all legacy data that contains credit card data, such as a cardholder's Primary Account Number (PAN) from all network computers. You must also ensure that any legacy cryptographic keys are securely deleted. The secure deletion and then wiping of data are requirements of PA-DSS.

Legacy data includes, but is not limited to, neglected and/or forgotten data on stored zip or other media backups, data on computers that have been replaced, data copied to perform computer upgrades or to set up additional stations, and data copied for system maintenance.

Legacy data also can include imprints of credit cards taken at check in, faxes with credit card guarantee information, and/or printed copies of past reports including night audits.

This document addresses legacy data, which is not part of the PMS active data that may reside on any of your computers.

The Customer's network administrator should use caution when performing the secure data deletion and wiping. If the Customer or network administrator is in doubt about any step, please contact AutoClerk Technical Support at (925) 284-1005 or AutoClerk President Gary Gibb at (925) 871-1801.

Background

The AutoClerk program has integrated features for purging old data backups, but the automated purging process only works on the backups in specific directories on the hotel's AutoClerk server or the AutoClerk station #1. A common and dangerous practice when doing a computer hardware upgrade is to use an existing computer as temporary storage for a copy of the old files. When the new computer is installed on the network, the old files are bulk copied to the new computer, but rarely are the files wiped from the temporary storage computer. Such actions compound a data problem because the end result is that multiple computers have legacy data on them. The solution is to securely

delete any legacy data before any other data is transferred. You must then wipe the storage computer's disk once the transfer is complete.

When your property was updated to AutoClerk's Version 7, data within the active AutoClerk dataset was encrypted. It is the Customer's responsibility to follow the instructions detailed below to ensure that no legacy data resides on *any* computer (server, computer, or laptop) outside of the active AutoClerk dataset.

File Removal Basics

If you need to log onto a computer with administrative rights in order to access and securely delete data you *must* log off when you are done to prevent others from using the computer with administrative rights.

When you are finished removing files from a given computer, you *must* include all users' Windows recycle bins in a wipe of the system. Windows will automatically re-generate a recycle folder when needed in the future.

When you have securely deleted all legacy data from a computer, you *must* wipe the drives using a wipe tool program. Two programs that some of our properties have used are Eraser http://heidi.ie/eraser/ (free) and CyberScrub's Privacy Suite http://www.cyberscrub.com/ (for a charge). These tools “wipe” or overwrite data in the computer's unused or empty space to make it unreadable.

AutoClerk's Data Conventions

A Customer only has one active working AutoClerk dataset. It resides on the property's AutoClerk server computer (be it dedicated or non-dedicated). It is always within a directory called, “autoclerk,” which is located on one of the AutoClerk server's root drives.

To protect against data loss, compressed backup copies of the active dataset are automatically created whenever a shift change or night audit is performed on Station #1. Dataset backups are comprised of three compressed zip files: data.zip, profile.zip, and xdev.zip.

All compressed backup files should reside *only* on the AutoClerk server and on Station #1, within specific directories (...\autoclerk\backup). They should always be current, less than one month in age. No other computer should have *any* uncompressed or compressed AutoClerk data files.

Uncompressed copies of an AutoClerk dataset and compressed AutoClerk zip backups more than 1 month old must always be securely deleted whenever and wherever found.

Your network administrator *must* perform an all-inclusive search to locate all PMS dataset copies. One way is to search is as follows: at the command prompt on each local drive's root directory (e.g. c:\, d:\, etc.), type: dir data.zip /s /p. Take the same steps for profile.zip and xdev.zip. This shows you all directories in which data.zip resides, and possibly where other encrypted or unencrypted legacy data files are. All copies of these files must be securely deleted.

For Station #1's that are standalone, peer-to-peer, or are *not* user-profile enabled, the automated backup files in c:\autoclerk\backup should not be older than one month.

For user profile enabled computers that are part of a dedicated server network, the directory c:\autoclerk should be entirely deleted. Do *not* delete c:\autoclerk on the AutoClerk dedicated server. Backups should only be on Station #1's %allusersprofile%\application data\autoclerk\backup directory and should not be more than one month old.

Credit Card Initialization File

On each computer, including the AutoClerk server, search for a file: psdf.pf1. It should only be found on the AutoClerk server's data\credit folder, and should have a current date. Any other instances must be securely deleted.

Log Files

All AutoClerk client log files must be securely deleted. On all computers, search for and securely delete log files beginning with “ac”. They will be followed by a number.

Do *not* delete any as*.log files as these contain important user log information which *must* be retained, per PCI DSS.

On computers that are running AutoClerk Central Reservation System (CRS) interfaces (such as AutoClerk's ResOnTheWeb service, or other third-party CRS vendors), it is important to securely delete the CRS interface log files. These interfaces run on the server and the log files are in the Windows temp directory. Examples of these files, all of which are ".log," have the following prefixes: row, hub, topz, syx, grs, tvc, uz, rw, hope, and bw.

Interface log files for the various CRS interfaces contain data such as guest name, arrival, and departure. If more than a few dozen CRS log files are found, contact AutoClerk's Technical Department and have them modify AutoClerk's Acmaint's Configuration files, so the deletion of old CRS log files is automatic in the future.

Securely delete all CRS interface log files in the temp directory. Remember not to delete *any* log files that begin with “as”.

Other log files can be maintained as they will now be automatically purged by AutoClerk program “Acmaint” and/or do not contain any sensitive credit card data.

On the AutoClerk server's drive that has the active AutoClerk data (which may not be the c: drive), securely delete the following: cclog.2004*.*; cclog.2005*.*; cclog.2006*.*; and cclog.2007*.*; etc., from the data\credit directory.

Other Miscellaneous Search and Destroys

You will need to do a few more searches before you run a wipe utility. This is because the AutoClerk PMS only maintains its own active data, not legacy data or data that resides outside the active data. If you find any of the files listed below, you must securely delete them, and as a last step, perform a wipe.

AutoClerk PMS historical folio files can be found by searching for the first three characters of the month, followed by an asterisk, then .txt, for example: jan*.txt. The asterisk will be the year.

Search for files with a .pf1 or .is1 suffix.

Search files for ac2g. Keep in mind that it may be named as follows: oldac2g.exe, ac2gold.exe, ac2g.old. The AutoClerk client executables may contain legacy cryptographic; therefore, all variations of this executable must be found and securely deleted.

Search for AutoClerk's p-system data which will be in a directory: rec. If you find the directory rec, and under it are such things as bios.rec, config.rec, sys.vol, then delete the entire rec directory.

These tasks must be performed on all property computers regardless of whether or not they are still in use and/or process credit card transactions. In addition, you must use a wipe tool on each computer after any secure deletion is completed.

Remember, not securely deleting the legacy data and then wiping the drives makes you *non*-PCI DSS compliant. You must follow your property's data retention policy, in regards to keeping, accessing, and subsequently deleting and/or destroying credit card data.

You may wish to destroy the media that legacy data is stored on. One way to destroy removable media such as zip disks is to reformat them and then scrub the magnetic surface. You can also physically destroy the media by drilling a hole through the magnetic surface and/or taking them apart to expose the magnetic disk, which must then be cut with scissors. In the case of printed reports, you can securely destroy the reports using a shredder that implements crosscut shredding.

Appendix B: System Specifications

Note for all systems: Each user must be configured with their own standard Windows user with a “complex” password, in that they must contain at least 7 characters and include both letters and numbers. Passwords can be even more secure by including upper- and lower-case letters and/or special characters.

Those employees that need administrative level access to a computer must have a separate user and “complex” password with administrative access, which must only been used when that access level is needed.

All customers and integrators are strongly advised to control access, via unique user ID and PCI DSS-compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data. (PA-DSS 3.2)

Restore points must be disabled on all systems.

All users must be set to time out after 15 minutes of inactivity. (PA-DSS 3.1.10)

AutoClerk Minimum Requirements for a Single Computer

Computer running Windows 7 Professional (SP1) or Windows 8.1 Pro

Anti-virus software

Intel Processor 2.0 GHz

4 GB Ram

Video Supporting 1024 x 768

Network Interface Card – Must be 3Com, Intel or Broadcom (1 GB)

Hard drive 40GB Disk storage available for AutoClerk.

Color Monitor

Keyboard

Mouse

Speakers or Headphones (For instructional Videos)

DB9 RS232 Serial Port - One is needed for each of most interfaces. Digi or Edgeport for multiple Serial Ports.

Laser Printer (must be local or network).

Dedicated USB Port

USB Printer Cable

Battery Backup

High Speed Internet Access with a Static IP address

Properly configured hardware systems for AutoClerk can be directly purchased from Technology At Work.

AutoClerk Minimum Requirements Non-Dedicated Server (4 stations max)

Two or more Computers running Windows 7 Professional (SP1) or Windows 8.1 Pro

Anti-virus software

Intel Processor 2.0 GHz

4 GB Ram

Video Supporting 1024 x 768

Network Interface Card – Must be 3Com, Intel or Broadcom (1 GB)

Hard drive 40GB Disk storage available for AutoClerk.

Color Monitor

Keyboard

Mouse

Speakers or Headphones (For instructional Videos)

DB9 RS232 Serial Port - One is needed for each of most interfaces only on the computer(s) running the interface(s). Digi or Edgeport for multiple Serial Ports.

Laser Printer (local or network)

Dedicated USB Port

USB Printer Cable

Battery Backup

High Speed Internet Access with a Static IP address

Network Switch (1 GB)

Category 5 (Cat 5) Cabling

Properly configured hardware systems for AutoClerk can be directly purchased from Technology At Work.

AutoClerk Minimum Requirements Dedicated Server. Required for 4 plus stations

Local Work Stations

Computers running Windows 7 Professional (SP1) or Windows 8.1 Pro

Anti-virus software

Intel Processor 2.0 GHz

4 GB Ram

Video Supporting 1024 x 768

Network Interface Card – Must be 3Com, Intel or Broadcom (1 GB)

Hard drive 40GB Disk storage available for AutoClerk.

Color Monitor

Keyboard

Mouse

Speakers or Headphones (For instructional Videos)

DB9 RS232 Serial Port - One is needed for each of most interfaces only on the computer(s) running the interface(s). Digi or Edgeport for multiple Serial Ports.

Laser Printer (local or network)

Dedicated USB Port

USB Printer Cable

Battery Backup

Remote Work Stations

Same as above but with Terminal Services. Terminal Server installed on a dedicated server.

Your network administrator should use a high level of encryption (128-bit key) when setting up Terminal Services. Be sure the data transmission is encrypted in both directions.

Dedicated Application Server with Primary Domain Controller

Microsoft Server 2008 R2 Standard (SP1) or Microsoft Server 2012

Anti-virus software

Intel Processor 2.0 GHz

8 Gig Ram

Video Supporting 1024 x 768

Network Interface Card – Must be 3Com, Intel or Broadcom (1 GB)

Hard drive 40GB Disk storage available for AutoClerk. It is highly desirable that redundant (RAID 1 or higher) disk storage be used.

Monitor

Keyboard

Mouse

DB9 RS232 Serial Port – One is needed for each of most interfaces. Digi or Edgeport for multiple Serial Ports.

UPS from APC with PowerChute

High Speed Internet Access with a Static IP address

Network Switch (1 GB)

Category 5 (Cat 5) Cabling

Properly configured hardware systems for AutoClerk can be directly purchased from Technology At Work.

Special Interface considerations:

Best Western Properties:

Best Western properties require a PMS-Router configured specifically for the Best Western 2-Way Interface.

Credit Card Processing:
Magtek USB Plug n Play Part No 21040110

Properly configured hardware systems for AutoClerk can be directly purchased from Technology At Work.

Appendix C: Sample Key Custodian Form

The following is a sample of the Key Custodian form that must be signed by all Key Custodians:

The signee of this document acknowledges that he or she has been afforded access to key management devices, software, and equipment. I understand I have been chosen as a key custodian for one (1) AutoClerk backup encryption key.

I hereby agree that I:

1. Have read and understood the policies and procedures associated with key management and agree to comply with them to the best of my ability. I have been trained in security awareness and have had the ability to raise questions and have had those questions satisfactorily answered.
2. Agree to never divulge to any third party, especially including personnel who maintain the other half of the key management or related security systems, passwords, processes, security hardware, or secrets associated with the AutoClerk system, unless authorized by a manager, owner, or required to do so by law enforcement officers.
3. Agree to report promptly and in full to the correct personnel, any suspicious activity including but not limited to key compromise or suspected key compromise. Suspicious activity can include the following: Phone requests from unidentifiable callers for access to secure information, unidentifiable files found on computers, and unusual activity recorded in log files.
4. My duties are to generate my half of the AutoClerk backup encryption key when necessary and to protect the integrity of this password at all times. If it is written down, then the written password must be secured within a secure, locked area, preferably a safe.

_____

Signature Date

_____

Print Name