# Appendix E: AutoClerk System Specifications

AutoClerk's goal is for your property to have a reliable and secure AutoClerk PMS installation. To ensure all AutoClerk PMS functions and capabilities perform as specified, please follow these steps.

Your network set up and installation must comply with the Payment Card Industry Data Security Standard (PCI DSS) version 1.2.1 of July 2009. The PCI DSS includes, but is not limited to: the firewall, antivirus programs, user accounts and their permissions, and physical and network access to the server.

You must make sure your computer/hardware/network administrator follows best practices with regards to network security. Your network administrator should hold current Microsoft Certifications, for example: Microsoft Certified IT Professional (MCITP). Having this credential does not give assurance of Information Technology (IT) competency, but it shows your vendor is keeping up-to-date with industry standards.

AutoClerk, Inc. requires the purchase of business-grade computers. This is important because the property operates 24/7 and many of the computers, especially the AutoClerk server, will also run 24/7. It is recommended that you select a hardware vendor who can provide support for the computers, network, operating system, and other software during the hours your property needs such support.

AutoClerk technicians will not install the AutoClerk software on computers that do not meet AutoClerk's Specifications. This can delay an installation and increase costs. To avoid costly repairs and delays, please be absolutely sure that your hardware vendor reads and follows the AutoClerk PA-DSS Implementation Guide and AutoClerk's “System Specifications”; you order the correct equipment from your vendor, and your vendor delivers and properly installs the equipment you ordered.

## General Installation Requirements

1. High-speed Internet access is required. It must be persistent and static and be accessible via a public (not private) address. Examples of acceptable broadband services would be: DSL, T1, or cable modem.
2. External Hardware Firewall (PCI DSS Req. 1): This is a dedicated device placed between your Internet connection and Local Area Network (LAN). It is not sufficient to rely exclusively on personal software firewalls co-resident on your LAN. Examples of software firewalls are: Windows Firewall, ZoneAlarm, BlackIce, and Panda. If present, software firewalls must be configured to allow AutoClerk internal LAN traffic (tcp/udp ports 11193). Shift4’s (credit card gateway) internal LAN traffic uses port 17477, and it uses tcp ports 26880 and 26881 for its outbound traffic. Depending on what, if any, Internet reservation interfaces you have with AutoClerk, additional(s) ports will need to be opened.
3. AutoClerk support uses a system/product called Bomgar which requires ports open for the hotel staff to get out on the Internet to initiate a support session. See Support - Establishing a Connection below for the necessary ports.
4. The 100 Base T Network Switch is made by one of the following manufacturers:
   - 3Com http://www.3com.com (Now part of HP)
   - HP http://www.hp.com

- CISCO http://www.cisco.com (including Linksys http://www.linksys.com)
- Edimax http://www.edimax.com
- Dell http://www.dell.com
- Netopia http://www.netopia.com
- Netgear ProSafe http://www.netgear.com/

In addition:

1. All equipment must be connected to mains power via a surge suppressor or an uninterruptible power supply (UPS) of sufficient capacity. All surge suppressors used should be supplied with an insurance policy.
2. Serial ports are RS232C with male DB9 connectors.
3. All serial interfaces require one serial port (RS232C DB9). Interfaces run on the AutoClerk server. If you are not sure how many interfaces the property is purchasing, please call your AutoClerk sales rep.
4. If you need to add a serial port, the AutoClerk approved extenders are as follows:
    - Digi board http://www.digi.com/products/multiportserialcards/index.jsp (Digi Neo for low profile solutions)
    - AccelePort Xr920
    - Ionetworks http://www.digi.com/products/usb/edgeport.jsp
    - Edgeport USB to multi port RS232C.
5. All system clocks must be synchronized (PCI DSS Req. 10.4). This is imperative for the Best Western 2 Way Reservation Interface.
6. Each station which processes credit cards must have a separate card swipe. It must be a MagTek MiniUSB Magnetic Stripe Card Reader: Part# 21040110.

## All Computers

All computers must meet at minimum, the following specifications. (Note: Dedicated servers have additional requirements that override those given here.)

1. Operating systems: Permitted OS include Windows 7 Pro 32-bit, Windows 7 Pro 64-bit, Windows 8.1 Pro 32-bit, Windows 8.1 Pro 64-bit.
2. Processor speed: Use Intel Pentium 4 or compatible processor, 1.3 GHz minimum.
3. RAM: You need 1 Gig RAM (minimum).
4. Video Card capable of supporting a display resolution of 1024 x 768 with 16-bit color.
5. Monitors: Monitor need to have a resolution of 1024 x 768 minimum. If it is a touch screen monitor, a serial port may be needed for the touch screen. Monitors may not be shared.
6. Keyboard and mouse: Use a standard keyboard and mouse. However, these may not be shared.
7. Network Interface Card (NIC): Use a 100mb/sec or Gigabit Network Interface Card (NIC) from these manufacturers:

- 3Com http://www.3com.com (Now part of HP)
- Intel http://www.intel.com or
- Broadcom http://www.broadcom.com/products/brands/NetXtreme

8. Anti-virus software: The software must be current, actively running and set to generate assessment logs (PCI DSS Req. 5.2). It should also be capable of detecting, removing, and protecting against other malicious software such as adware and spyware (PCI DSS Req. 5.1).
9. Screen savers and computer lock-out screens: Set screen savers and computer lockout to require a user to re-enter their password to re-activate the terminal if it has been idle for more than 15 minutes (PCI DSS Req. 8.5.15).
10. Speakers or headphones: AutoClerk's Video Training modules require speakers or headphones. (Speakers may not be necessary on all computers; just those that the property wants their staff to use AutoClerk's training modules on.)
11. User names and passwords: There must be unique user names and passwords for all users (PCI DSS Req. 8). (See the section in this system specification, "Installation" for more details on users and password requirements.)
12. Browsers: A browser must be installed in order for staff to see reports within AutoClerk.
13. If the Internet is blocked on computers, you must allow access to esupport.autoclerk.com so the property can get support from AutoClerk. Staff will also need the ability to download an applet for the support session. You should also consider allowing access to http://www.autoclerk.com and http://www.myautoclerk.com.

## Dedicated Server (Required for our Best Western Customers)

AutoClerk recommends that ALL properties have a dedicated server network. If you are an existing AutoClerk client and do not have a dedicated server network, consider switching to one. It will provide better security and system dependability. A dedicated server network can better support strong enterprise-level enforcement of operating system, anti-virus and anti-spyware updates, while keeping user stations restricted to non-administrative access. If you are a Best Western (BW) property, a dedicated file server is required.

If your computer set up is one or two computers, then you do not have to have a dedicated server. However, if you have three (3) or more stations and/or you are a Best Western property, you MUST have a dedicated server network.

AutoClerk's Specifications for the AutoClerk dedicated server are:

Note: If a specification is listed above for ALL computers, then it also applies to the dedicated server, unless a variation and/or addition is listed below.

1. Microsoft Windows Server 2008 R2 Standard (SP1) or Server 2012. You can use Windows 7 Pro 32-bit, Windows 7 Pro-64-bit, or Windows 8.1 Pro 64-bit ONLY if the server network has three or fewer AutoClerk stations. Intel Pentium 4 or compatible processor.
2. CD-ROM or DVD drive
3. 20GB Disk storage available for AutoClerk. It is highly desirable that redundant (RAID 1 or higher) disk storage be used. It may be SCSI or Serial ATA.
4. A server class Smart UPS with messaging enabled.

5. A serial port extender as specified above may be required depending on how many serial interfaces the property is purchasing.
6. The server must have a keyboard, mouse and monitor but cannot share them with a workstation.
7. Speakers are not necessary for a dedicated server.
8. If the property is getting the credit card interface through AutoClerk, they MUST use Shift4, a payment gateway. (More on credit cards and the interface below.)

Station #1 and any station designated as a backup station #1

If you have an AutoClerk dedicated server, Station #1 is your main AutoClerk station. If you only have 1 or 2 stations and are opting to not have an AutoClerk dedicated server, then Station #1 will also act as a non-dedicated server. In both cases, Station #1 is usually located at the front desk. These are additional requirements for Station #1 (and the designated backup #1 only)

1. 20 GB Disk storage
2. CD-ROM or DVD drive
3. UPS

## Credit Card Data Capture Security Requirements

ALL hoteliers that store, process and/or transmit confidential credit cardholder data, regardless of whether or not they process credit cards through AutoClerk MUST comply with the PCI DSS Requirements found at: https://www.pcisecuritystandards.org. A summary of the current requirements are:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for employees and contractors

If a property is purchasing the credit card interface through AutoClerk, they MUST USE Shift4, a third party payment gateway provider. For Shift4 pricing and ordering, contact Bob Arsenault, Manager of Business Development-Hospitality at Shift4, 702-597-2480, x43106, or barsenault@shift4.com.

Notes:

AutoClerk does not endorse other application programs such as Microsoft Office or system services such as IIS, Apache or MSSQL, and cannot determine whether or not they may cause any incompatibilities.

If you choose to run other programs on a computer that is also running AutoClerk, you may need to increase RAM and disk capacities.

The primary front desk computer (Station #1) and the AutoClerk dedicated server, if you have one, are critical computers. Most properties require these computers to function 24 hours a day, seven days a week. These computers are responsible for creating a proper backup of hotel data.

Business grade computers and other business grade components must be used throughout the system. Consumer grade computers as found in many discount stores are NOT suitable. Computers with Windows XP Home Windows 7 Home or Media edition pre-installed are not business grade computers.

## Installation Specifications

### Network

While this section is aimed at dedicated server networks, the AutoClerk PMS program is a client/server application. Even on a single computer, many parts of AutoClerk act as a network. Please make sure you cover all portions of this section.

It is the responsibility of the hotelier to establish, ensure and maintain their own security in regards to not only the physical access to computers but to the data and in particular, the credit card data through the network.

To view a PDF of our Network Topology, go to http://www.myautoclerk.com/ and look under the Specifications header.

1. Cabling CAT 5E (Minimum) - Cabling is the most critical part of any network. AutoClerk requires that all network cabling be wired to the Category 5E (minimum) specifications as defined by the EIA/TIA-T568-B standard.

If the property already has cabling in place, have your network administrator scan the line with a 1 GB CAT 6 Cable Certification Scanner. If the cabling passes at CAT 5E performance or better, have the administrator sign off on the scan certification and retain it at the property. If not, then make the necessary changes.

Sub-standard cabling is very difficult and expensive to diagnose. Many times it will start out fine and decay over time. When it does have problems, the problems may mimic other types of software and hardware problems.

AutoClerk requires that the entire cabling hardware AND installation specifications be followed. This includes, but is not limited to:

- The quality of the cable
- Cable runs must be from a "Patch Panel" at the server location to a jack at the station locations.
- RJ-45 Patch Cords must be used to connect the actual computers to the jacks and patch panel.
- Patch Cords must be machine pressed. No handmade patch cords. No ‘Home Runs’.
- Cable runs must avoid appliances that can cause interference such as florescent lights.

- Jacks must be punch down, no screw connectors.
- Jacks and the Patch Panel are to be clearly marked and a wiring diagram posted at the server.

2. Wireless - Wireless connections to the AutoClerk network segment must NEVER be used.

   If your property has ANY type of public wireless Ethernet accessibility, such as from guest rooms, it MUST be on a separate network segment. In addition, you MUST follow PCI DSS Reqs. 2.1.1 and 4.1.1. These requirements include but are not limited to configuring a perimeter firewall to deny traffic from any public access wireless environment to the AutoClerk Client environment; not using any default WEP keys; not using any default passwords; and enabling WPA technology, if applicable. (See Section 6 of the Implementation Guide for more information)

3. Network Switch - AutoClerk requires the network to be at least 100 Base T. If the AutoClerk dedicated server should fail, the PMS is designed so the server program can be installed on another computer and the network can continue to operate while the server is being repaired or replaced as long as the network switch and cabling are intact. The network switch must be plugged into the UPS so it will continue to function during a power outage.

4. Power, UPS and Smart communications - Computers will not run without power, and will not run well without proper power.

   Like cabling, clean power is critical! Each computer must have clean power. The file server must have a dedicated line with an isolated ground.

   Station #1 must have a battery backup (UPS). Make sure all components of Station #1 are plugged into the battery. (CPU and monitor. Laser printers may overload a UPS and therefore should not be plugged into it.) Printers should be plugged into a surge protector. Some UPSs have surge protector outlets that are not UPS protected.

   The AutoClerk dedicated server requires a UPS with Smart messaging software. All components (CPU, Monitor, Network Switches ...etc) must be plugged into this UPS. APC and PowerChute have proven to be reliable and our staff is familiar with these products.

   As batteries age, the amount of power and the amount of time they can provide emergency power declines. The typical life expectancy is about 3 years. This life expectancy can be substantially shortened if the battery is used often. Depending on the quality of the power in your area, you may want a larger capacity UPS and may even need to consider installing a line conditioner to assure that the power is clean.

5. Server Location - The AutoClerk server must not be located in a heavy traffic area. It should be in a well ventilated, easily accessible but locked cabinet or rack. As your credit card data is transmitted through the server, you MUST restrict and control physical access to the server location. (PCI DSS Req. 9)

6. Server Operating System (If dedicated on a network of three (3) or more computers) - Must run Windows 2008 64-bit Server Edition or Server 2012, as a Primary Domain Controller. Set it to automatically download updates so the system always has the latest updates and patches. Installation should be managed by your network administrator.

7. Drive Mapping - AutoClerk requires a "V:" drive map, sharing the AutoClerk Client install bin directory.

   a. AutoClerk will be installed in the file server's largest hard drive partition.

   b. Right click on the directory /autoclerk/bin and share it as "autoclerk"

c. Click on the "Permissions" button and set as follows:

d. Everyone = read only

e. This is the ONLY AutoClerk directory that users can see

8. We suggest using a Domain Login Script called otto.bat to set the drive mapping with the contents:

   net use v: \\192.168.0.100\bin /p:y

   If this is a Peer to Peer network, or a dedicated server running Windows 7 32-bit, Windows 7 64-bit, or Windows 8.1 Pro 64-bit then on the non-sever station(s), we suggest you map the drive by creating an autostart.bat file to be placed in the all users startup folder. The contents should be: net use v: \\192.168.0.100\bin /p:y

9. User Accounts - Administrator(s)

   Create an Administrator user with a unique user name and complex/strong password. Do NOT use any vendor supplied defaults for any system passwords or other security parameters. (PCI DSS Req. 2) See section 'k' below for password requirements for ALL users. Make sure the hotel's General Manager/Owner knows the Administrative user name and password.

   Create another administrative user, again with a unique user name and complex/strong password that will ONLY be used by AutoClerk. Call AutoClerk (925-284-1005) with that user name and password. AutoClerk technicians will need it to install our software and interfaces. Once the AutoClerk installation is complete and ALL interfaces have been installed and tested, you MUST disable that account. The account must be re-enabled "only when needed..., and monitored while being used". (PCI DSS Req. 8.5.6)

   Property management must either disable or not use ANY users with Administrative rights on a day to day basis. (PCI DSS 8.5)

10. User Accounts - Everyone

    ALL USERS MUST HAVE THEIR OWN UNIQUE ID (PCI DSS Req. 8)

    Get a list all current users from the hotel General Manager and set them up in Windows with a unique user name. These users must NOT have administrative rights. There must be an additional method of login authentication. Accepted methods include: a password, a token device or biometrics. If the property chooses to use passwords, then the passwords MUST follow the requirements listed below.

11. Password Requirements

    a. any vendor supplied defaults must be changed prior to installing a system on the network (PCI DSS Req. 2.1)

    b. control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

    c. verify the user's identity before resetting a password

    d. set first-time passwords to a unique value for each user and set so it must be changed immediately after the first use

    e. revoke access for any terminated users immediately upon their dismissal

    f. remove any inactive user accounts at least every 90 days

    g. enable accounts used by vendors for remote maintenance only during the time period needed

h. hotel management must communicate password procedures and policies to all users who have access to cardholder data

i. do not use any group, shared, or generic accounts and passwords

j. change user passwords at least every 90 days

k. contains at least 7 characters

l. contains both letters and numbers

m. cannot duplicate any of the last 4 passwords

n. lockout ANY user after 6 failed attempts. This includes an administrator.

o. set the lockout duration to 30 minutes or until an administrator enables the user ID

p. if a computer session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

q. authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

12. Assign Login Script to Users - this is so the v: drive is mapped when they log onto stations and can use AutoClerk.

13. Disable Automatic Logon - Windows allows you to automate the logon process by storing your password and other pertinent information in the Registry database.

    Automatic logon MUST be disabled on EVERY computer on the network. In addition, if a computer session has been idle for more than 15 minutes, require the user to re-enter their Windows user and password to re-activate the terminal. (PCI DSS 8.5.15)

14. Windows Components - On the AutoClerk server running Windows 2008 64-bit OS, you must disable all unnecessary and insecure services and protocols. You must also remove all unnecessary functionality. (PCI DSS Reqs. 2.2.2 and 2.2.4)

### Workstations

1. All non-server network computers must use Windows 7 32-bit OS, Windows 7 64-bit OS, or Windows 8.1 Pro 64-bit. Ensure your network administrator is managing the OS updates so the system always has the latest updates and patches by enabling automatic downloads. (PCS DSS Req. 6)

2. Check for maverick applications. (PCI DSS Req. 2.2)

3. Make computers as basic as possible. Remove all icons from the desktop except 'My Computer', 'Network Neighborhood', and 'Recycle'. Consider a desktop lockdown policy.

4. Install anti-virus software on all computers. (PCI DSS Req. 5) Be sure the anti-virus programs are capable of detecting, removing, and protecting against other forms of malware. Also be sure the programs are current, actively running, and capable of generating assessment logs. They must be set to automatically update so they are always current with the program patches.

5. Remote AutoClerk stations (also known as Regional PMS) MUST be via Windows Terminal Services. When implementing the remote stations, be sure to follow best practices. Best practices includes but is not limited to: proper implementation of the hardware and personal software firewalls (PCI DSS Reqs. 1.1.3, 1.3), not using any vendor supplied defaults (PCI DSS Req. 2.1.1), implementing session timeouts, idle

timeouts, using non-standard RDP ports wrapped in a VPN tunnel and enabling auditing/logging.

You should always use a 'high' level of encryption which encrypts data transmission in both directions using a 128-bit key for Terminal Services.

Two-factor authentication must be used when connecting to the AutoClerk network segment from a remote station. Two factor authentication requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors. (See PCI DSS Req. 8.3 for more details)

Review PCI DSS Req. 12.3 for additional restrictions for remote access such as not allowing cut and paste. Refer to the Remote Access document on http://www.myautoclerk.com under Specifications for more information.

AutoClerk recommends you use VPN or SSL/TLS for encryption on your terminal server as you must "Encrypt all non-console administrative access." (PCI DSS Req. 2.3)

6. Disable or remove any unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, unencrypted FTP, and others).

### TCP/IP

Set individual (static) TCP/IP addresses for each computer as 192.168.0.N, Subnet Mask 255.255.255.0.

N is replaced by the number:

Server, N = 100.

Station 1, N = 101;

Station 2, N = 102, and so on.

The Server and Domain should have unique names for each property. In addition, each computer must have a unique name. HOTELNAME_SRVR, STATION1, STATION2, etc. is a good naming convention. The names may NOT have spaces.

Test for TCP/IP connectivity on every computer.

## AutoClerk Data Backup

The AutoClerk PMS backs up AutoClerk data, storing a copy on the internal hard disk of the AutoClerk server in c:\autoclerk\ [hotelid]\backup. It also places a copy of the backup on the internal hard disk of Station #1 in C:\Documents and Settings\All Users\Application Data\autoclerk\backup. These backups are performed by default at each shift change and during the night audit.

The AutoClerk night audit can send an additional copy of the backup to removable media attached to Station #1.

You MUST discuss options with the hotel's management if they would like this option and if so, what will be used. You may use any backup device of hotel management's choice, excluding optical drives. The hotel's network administrator, and not AutoClerk, is responsible for supporting removable media backups. Removable backup is disabled by default.

AutoClerk has an option to place a data backup on an extra directory or drive on the hotel's dedicated server or Station #1. This extra location may be an internal or external device,

but must be referenced as a drive letter or path (no UNC) from Station #1. The default location will be c:\autoclerk\ [hotelid]\backup\extra. The 'extra' backup is in lieu of the removable backup, and takes place during the night audit. We strongly suggest the contents of this extra directory/drive then be copied by any third party backup software product of hotel management's choice and stored offsite. An extra backup is disabled by default.

While there are many different third-party backup software solutions, AutoClerk provides a proven IP Backup solution. AutoClerk IP Backup is available as and additional service. Please contact AutoClerk for more information.

The AutoClerk PMS automatically performs rolling purges of the AutoClerk backup folders on a nightly basis after a backup file has aged beyond a certain set point, as determined by hotel management. The number of backups kept on the drive is configurable.

Warning: If hotel management chooses to have no zip disk backup AND also chooses to have no other external backup service or removable media, the hotel is at risk of catastrophic data loss in the event of a hard disk crash (on the server and/or station #1).

## Printers

A laser printer and AutoClerk's plain paper registration slips and folios, also known as stylesheets, are required for use with AutoClerk.

There must be a default printer configured on Station #1. This printer will be used for night audit.

Printers should be connected directly to the network via TCP/IP. Any printer connected via USB will be for local (NOT shared) use only.

## AutoClerk Support

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 they are working at, and entering a 7 digit pin code our support agent will give them over the phone. That pin is only good for that support session
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, or others. If the property is interested in having this installed, please contact AutoClerk Technical support at (925) 284-1005 during regular business hours.

### Establishing a Connection

A browser MUST be installed in order for staff to access the Internet to then get interactive support from AutoClerk staff. If the Internet is blocked on computers, you MUST allow access to esupport.autoclerk.com. Staff will also need the ability to download an applet for the support session.

Bomgar solutions are designed to work transparently through firewalls, enabling a connection with any computer with internet connectivity, anywhere in the world. However, with certain highly secured networks, some configuration may be necessary.

- Ports 80, 443, and 8200 need to be open for outbound TCP traffic.
- NOTE: Port 8200 is used as a rollover for port 443 and is not strictly required, though it is recommended.
- Internet Security software such as software firewalls must not block Bomgar executable files from downloading. Some examples of software firewalls include MacAfee Security, Norton Security, and Zone Alarm.
- If you do have a software firewall, you may experience some connection issues. To avoid such issues, configure your firewall settings to allow the following executables, wherein {uid} is a unique identifier consisting of letter and numbers:
    - bomgar-scc-{uid}.exe
    - bomgar-scc.exe
    - bomgar-pac-{uid}.exe
    - bomgar-pac.exe
- If you should still have difficulty making a connection, contact Bomgar support:
    - Toll-free: 1.877.8BOMGAR x2
    - International: +01.601.519.0123 x2
    - Email: SUPPORT@BOMGAR.COM

### Architecture

The architecture of Bomgar solutions lends built-in security to the support process. Because session traffic is outbound from both directions, both the customer and the support representative can work from behind corporate firewalls providing a barrier to any potentially malicious traffic.

In addition, each Bomgar session is initiated by the remote customer when the support issue occurs and is then discontinued automatically when the session is complete, allowing only a small, irregular period of time wherein Bomgar traffic is crossing the Internet. This secure architecture provides the first level of Bomgar security, obscuring the entire support session by leaving existing security structures in place and spontaneously generating each support session.

### Bomgar Box

Bomgar accounts and sessions interface with the Bomgar Box, which offers an extremely high level of security within a managed environment. All traffic passing through the Bomgar Box is 256-bit AES SSL (Secure Socket Layer) encrypted along the entire data stream. This encryption is in addition to the heavy data compression inherent in Bomgar traffic. The login pages for the Bomgar Box /appliance interface and /login administrative interface are 256-bit AES SSL encrypted and password-protected, preventing unauthorized users from accessing representative or administrator accounts.

## Network Administrator Responsibilities

As the property's network administrator you are responsible in training ALL staff on the following:

1. How to properly startup the system and log into the network.
2. How to properly shut down the system and the network.
3. Label and show them where all components of the system are including, but not limited to CPU, Monitor, UPS, Server, Network Switch, and Cable connections.
4. Windows Basics including but not limited to logging onto a computer, mouse use, active window, switching windows, and displaying the taskbar.
5. All non-AutoClerk programs. I.e. Word, Excel
6. How to check the battery level on the UPS.
7. How to set up, delete, enable, disable and maintain Windows users and authentication.

While AutoClerk is the first point of contact for all AutoClerk related problems, you will be called upon when needed to provide support for the following:

1. Hardware
2. Operating system
3. Network Communication(TCP/IP) Problems
4. Non-AutoClerk programs (I.e. Word, Excel, Internet)
5. Printing
6. Data Security

If AutoClerk determines that you need to be brought in, the customer will normally contact you directly. You should then contact us, and we will go over the problem together and lay out a plan of attack. The idea is that by the customer calling you, you know you have the authorization needed to act. By talking to us, rather than the customer, you get accurate information on a technical level and the customer is not brought into the middle.

Should the customer contact you directly to work on the system, even if it seems non-AutoClerk related, we must be contacted ahead of time so we can determine if an AutoClerk technician will need to be available or is required. Upon arriving at the property, we need to be contacted so we can make sure proper steps are done to assure the smooth operation of the property. Once finished, contact us again, so we can run tests to make sure AutoClerk is running properly.

## Security

As the network administrator, you are responsible for supporting the property's data security as stated in the PCI DSS. This includes but is not limited to:

1. Antivirus - Many of our customers use McAfee or Norton. (ALL computers on the network MUST have an antivirus program installed. It must be kept running at all times, and be enabled for automatic updates to ensure they are current with security patches. They must also be capable of detecting, removing and protecting against other forms of malware.(PCI DSS Req. 5)
2. Internet Firewall - AutoClerk requires a hardware firewall, however if you enable a software firewall in addition, then port 11193 MUST be opened in order for AutoClerk to run. (PCI DSS Req. 1)
3. Physical security of the dedicated server, if used. (PCI DSS Req. 9)
4. Regular testing of the security of the entire network (PCI DSS Req. 11)

5. Internal network security, including, but not limited to unique user names and passwords for ALL users; password rules and maintenance; user permissions; and enabling logs to track access.

The property's PCI DSS compliance depends, in part, on the set up and installation of the network hardware and software. Deviation from the above Specifications will make the property NON-PCI DSS compliant as well as vulnerable to breaches. It is the property's responsibility to see that their system is set up and installed in a PCI DSS complaint manner and that it is maintained to continue its compliancy.