

**Radiant Systems**

**Security Maintenance  
Recommended Standard  
Operating Procedures for  
Aloha POS**



## Security Maintenance Recommended Standard Operating Procedures for Aloha POS

The following checklist provides a list of Radiant Systems recommended standard operating procedures that should be completed and validated to enhance the security of our solutions at a customer site. These tasks are intended to be a high-level checklist and do not include instructions on how to execute tasks. Details on how to execute each task related to a specific Aloha POS solution can be found in the associated *Data Security Handbook*.

**Note:** PCI compliance is ultimately the responsibility of the customer. Although implementing the following security recommendations will help enhance the data security at a customer's site, it does not imply that they will be PCI compliant. If customers request assistance in helping to ensure the security of their site systems, conduct as many of these procedures as possible and note the disposition of each at the time that these activities are completed.

The following areas are covered:

- Windows/OS Configuration
- Remote Access Configuration
- Network Configuration
- User Management
- Audit
- POS Configuration

## **Windows/OS Configuration**

- Verify the version of operating system(s) in use are actively supported and considered compliant with industry standards.
- Ensure all critical updates or patches are applied to firmware, BIOS, drivers and operating systems.
- Ensure Windows is configured to purge the paging file at shutdown.
- Enable Windows firewall.
- Enable the audit logging features in Windows.
- Disable unnecessary services.
- Configure File Integrity Monitoring (FIM)
- Configure time-synchronization for all non-domain controller or domain member file servers and appropriate configure POS time synchronization.
- Ensure Windows System Restore is disabled on the Radiant PC/server and on all terminals to prevent Windows from saving sensitive information as part of the routine system-restoration process.
- Ensure Windows Remote Desktop is disabled if not needed or configured in a manner that meets secure implementation guidelines.

## **Remote Access Configuration**

- Ensure all default passwords are removed from the remote access software and use unique and complex passwords for each customer.
- Ensure there is a mechanism in place for rotating passwords on a regular basis.
- Ensure encrypted data transmission is enabled on the remote access software.
- Ensure account lockout after a certain number of failed login attempts is enabled.
- Ensure all connections are initiated and managed by the on-site user and only enabled when needed. Remote access tools should not be left in a listening mode.
- Ensure there is a mechanism for forcing automatic logoff after predetermined time of inactivity.
- Ensure the logging function on the remote access software is enabled.
- Limit remote connections to specific known IP/MAC addresses.
- Review default configuration settings and changes to comply with secure implementation guidelines and ensure connection is running over a secure protocol such as a Virtual Private Network (VPN) connection through a firewall. Examples of remote access tools can include, but are not limited to:
  - PC Anywhere
  - RDP (Terminal Services)
  - LogMeIn

## Network Configuration

- Ensure a hardware network firewall device is installed between the POS and the Internet.
- Ensure all non-POS related computers have personal firewall software installed.
- Ensure the firewall is configured to log and limit connections and access per secure implementation guidelines.
- Document and maintain a list of firewall rules to be used for auditing purposes.
- Limit inbound and outbound traffic to ports and IP locations (URLs) that are for business purposes only.
- Ensure antivirus/anti-malware software is installed and up to date on all POS end points, which include terminals, servers and workstations.
- Ensure unused network protocols are disabled.
- Scan hard drives for the presence of unencrypted cardholder data and securely delete any data or unallocated space using a secure wipe program in accordance with industry-accepted standards for secure deletion so that cardholder data that may be present cannot be reconstructed. Examples of secure wipe programs include but are not limited to:
  - DelTrack – (Aloha specific)
  - Eraser
  - sdelete
- In accordance with business needs and customers data retention policy, configure DELTRACK to remove historical credit card data after a specified number of days.
- Where applicable, ensure file sharing permissions are restricted to the user accounts that require access and limit based on the need to read/write versus read only.
- Enable an Intrusion Detection System (IDS).
- Enable Network Address Translation (NAT).
- Ensure no unapproved wireless devices are attached to the POS network segment; inventory all network devices for auditing purpose or install a wireless monitoring system to alert of unknown connections.
- When using wireless, ensure industry best practices are followed for a secure configuration (to include WPA2 and MAC-only assignment).
- Link documented customer business practices network configuration choices to justify the configuration.
- Create a network diagram for the configuration.

## **User Management**

- Create and configure unique user accounts for each POS terminal using complex passwords with 90 day (or less) password rotations; using the latest version of Radiant Application Loader can assist with POS user account administration.
- Create unique user accounts with complex passwords and 90 day (or less) password rotations for each user who needs access to the Back of House (BOH) file server or other workstations connected to the POS network; complex passwords are seven characters or longer containing a mixture of upper and lower case characters with numbers and/or non-alphanumeric characters, does not contain any part of the user name, and has not been used as any of the prior four passwords.
- Set first time passwords to a unique value for each user and configure to prompt for change at first use.
- Configure systems to limit user account exposure to automated brute force attacks by limiting repeated failed login attempts to six (or less) and locking out users for 30 minutes (or more) once the failed attempts threshold has been meet.
- Based on operating needs, configure systems to automatically lockout logged in users after a period of inactivity, requiring account and password validation upon return.
- Remove any unnecessary user accounts including those provided by third party vendors; where vendor accounts are required, ensure they are using complex passwords that follow 90 day (or less) password rotations.
- Revoke access for any terminated users.

## **Audit**

- Ensure Windows audit logs are reviewed on a periodic basis.
- Periodically review firewall configurations to documented settings.
- Periodically review network traffic activity to ensure no unknown devices are connected to POS segment and no unknown ports or IP addresses are being accessed.

## **POS Configuration**

- Securely remove historical data and logs and any non system generated files that may have been used for troubleshooting over time, such as .bak, .tmp, .zip. etc.
- Securely remove files containing sensitive information that were created with a version not validated by the PA-DSS.
- Configure automatic purging of historical data according to store's data retention policy.
- Ensure a PAPB or PA-DSS validated version is running; highly recommend using a version that is compliant with PA-DSS v1.2 or greater.
- Configure credit card tenders to mask credit card numbers (PAN) and suppress expiration dates on all displays, receipts, vouchers and external reports or exports.
- Configure back office security rights and assign user level permissions in support of business functional needs in order to limit access to reports with credit card numbers (PAN).
- Create specific user accounts for POS services and configure services to logon using said accounts.
- Where applicable, ensure the use of compliant hardware for credit and debit processing where PIN, EMV or the like are required.
- Limit hardware connections to approved components required by the POS solution for data processing (such as cash drawers, printers, coin changers, display boards and the like; not to include personal USB drives or other none POS related equipment).
- Where applicable, re-grind known Aloha POS dated subfolders containing data from prior versions.