



PCC OTC Bulletin

May, 2008

P O S Release 5.4 is Available

Spring has sprung and so has the P O S Release 5.4, which is now available with exciting new features. More security! More functionality! FMS requires that you upgrade your existing P O S computer to Release 5.4. We will be unable to support releases older than P O S Release 5.4 after September 30, 2008. As stated in the November 2007 bulletin, you will be notified by phone or email once we are ready for your agency to upgrade to Release 5.4. Agencies will have the option of either downloading the software from ELVIS or receiving a CD by mail. Please allow approximately 30 minutes to download the file depending on your network speed. The Standard Operating Procedure (SOP) for Release 5.4 is available for download on the PCC OTC static website at: <https://www.pccotc.gov/pccotc/Downloads/r54sop.htm>.

This bulletin addresses the FISMA (Federal Information Security Management Act) compliancy efforts that necessitated the creation of the *SAT Appendix 1 - Security Best Practices* chapter. The new appendix is attached to this bulletin and should be printed and placed in your S O P as a part of the SAT chapter (Chapter 3). A recap of what is included in the Security Best Practices Appendix is included in this bulletin.

This bulletin also describes the changes and new functionality in Release 5.4 designed to enhance your use of the P O S software. The contents of Release 5.4 can be found at the end of this bulletin.

Security Best Practices

As mentioned above, a new *Best Security Practices - Appendix 1* for the SAT chapter of the S O P is attached to this bulletin. The document is written to provide security best practices for the PCC OTC system that guides agencies toward FISMA (Federal Information Security Management Act) compliance. It outlines points from the *NIST (National Institute of Standards and Technology) Special Publication 800-53*, which can be found at <http://csrc.nist.gov/publications/PubsSPs.html>. Each Agency's internal guidelines should take Treasury security best practices into consideration. Please refer to the *NIST Special Publication 800-53* and related publications for complete text of the 'Recommended Security Controls for Federal Information Systems'.

Some Security Best Practices include:

Access Control

- Examine P O S and ELVIS role and permission assignments. Access to the system should be granted at the lowest level available that still allows users to perform their job duties.
- Ensure that proper separation of duties exist. As an example, users that key in batch information should not have access to the SAT to add or edit users or make changes to configuration settings.
- Ensure that the maximum number of failed login attempts to the P O S computer has not been altered to a number higher than 3.
- Review and certify internal P O S users annually for each of your

computers. This is in addition to the annual review that is done by the FRB-C for the ELVIS application.

- Information stored on the PCC OTC's hard drive, secondary storage drive, and printouts may contain personally identifiable information (PII) in the form of names, account numbers, social security numbers, etc. within a P O S batch and therefore should be protected, physically secured, and accounted for.

Risk Assessment

Identify risks through a formal process and make a conscious decision to accept, mitigate, or avoid those risks. To assist agencies with risk assessment, a Business Risk Assessment template can be obtained from the PCC OTC static site at <https://www.pccotc.gov/pccotc/Downloads/download.htm>.

Personnel Security and Procedures

- Ensure that users read and understand the PCC OTC ‘Rules of Behavior’, ‘Privacy Statement’, and ‘Accessibility Statement’ which are available through links on the ELVIS sign-on screen.
- Ensure all PCC OTC hardware and software is no longer in the possession of exiting users.
- Ensure that exiting users are deleted from both the P O S and the ELVIS system.

Physical and Environmental Protection

- Control who has access to the physical area that houses the PCC OTC computer. To the extent that the operational environment allows, PCC OTC scanners and check processing should be done in controlled environments such as steel cages, cashier cages, behind glass windows, and within offices where access to the PCC OTC system and peripheral equipment can be physically controlled.
- Agencies are responsible for securing PCC OTC scanners, peripheral equipment, checks, and other sensitive information in locked rooms, locked cabinets, or security containers supported by appropriate key control and other physical security controls.
- Ensure that unauthorized users cannot view the computer screen of the PCC OTC computer.

Configuration Management

- Keep a current, documented listing of all PCC OTC hardware and software.
- Periodically check to ensure that the PCC OTC SAT configuration settings are set to the recommended defaults as follows:
 - Maximum failed Login attempt - 3
 - Auto logout – should be checked and inactive minutes set to 15
 - Batch Delete Age – 7 days (only 7 days of batches should be retained to reduce the amount of personal information stored on the hard drive of the P O S computer and its secondary storage device. Higher amounts of stored P I I data equates to higher risk of accidental disclosure in the event of unauthorized access to the system, or malicious code.)
 - Activity Log retention – 365 day(To view the SAT ‘System Configuration’ settings, an authorized user should sign on to the SAT and click the ‘System’ icon, then click the ‘General’ tab. See *SAT* chapter of the *PCC OTC S O P* for complete instructions)
- Only designated P O C’s (Point of Contacts) or security contacts should be allowed access to the PCC OTC SAT.
- Review the P O S activity log for suspicious activity.

System Maintenance

- Perform regularly scheduled maintenance on the P O S computer such as disk optimization tools, virus checking tools, etc., by authorized personnel.
- If a component needs to be removed for repairs, all sensitive information should be removed.

P O S Computer/Workstation Protection

- Ensure that only authorized users have access to the PCC OTC workstation.
- Label and store all removable media in a secured location. Removable media includes flash drives, CDs, zip disks and smartcards.
- Remove PCC OTC related data from drives prior to destruction or reuse.
- Shred PCC OTC paper output that contains sensitive information.
- Only authorized users should have access to the PCC OTC work area and output reports. This means all printouts, hard disks, LAN drives, external hard disks, diskettes, CDs, zip disks, smart cards, and USB flash drives.

Secondary Storage Protection

PCC OTC requires the use of a secondary storage device. This device is used to retain batch information and check images in the event of a computer failure or data corruption on the hard drive prior to transmission. Special precautions are necessary in order to safeguard the sensitive information that is stored on the secondary storage drive, especially if that storage drive is in the form of a USB flash drive, smartcard, zip disk or other compact storage device. These small, external media types are very compact and easy to lose or steal. The P O S provides a minimum level of encryption to the data stored on the secondary storage drive which may prevent unauthorized users to read the data. Agencies may also consider using additional levels of encryption to protect the data on the secondary storage drive. More information on additional encryption can be found in the *SAT Chapter - Security Best Practices Appendix 1* of the *PCC OTC S O P*, and section SC-13 of the *NIST Special Publication 800-53*.

Release 5.4 Enhancements

Listed below is a brief description of the enhancements that are included in the P O S Release 5.4.

Updated Password Policy

Modifications have been made to the password policy for the P O S. These changes have already been implemented for the ELVIS system and are now being incorporated into the P O S software. For complete information on password requirements, please see *Appendix R – Password Requirements* of your Release 5.4 S O P, which was sent electronically to all Agencies in November, 2007. If you need a copy of Appendix R, please contact the PCC OTC Customer Service staff.

Back Office Conversion

The Back Office processing method allows customers to convert payments received at the point-of-sale locations to ACH entries in a controlled, back-office environment. The new mode offers the following updates:

- ◆ A new “Back Office Conversion” mode on the P O S data entry screen to capture check items.
- ◆ CIRA query results and detail screens display the words ‘Back Office’ for the processing mode for all Back Office items.
- ◆ On the CSV Agency detailed item report, the check type and processing mode are indicated as ‘personal/non personal’ and ‘Back Office’ respectively.

Prior to using the ‘Back Office’ processing method, Agencies first need to download the compatible data entry screen. Complete information on how to download the data entry screens can be found in *Chapter 6, Daily Processing* of the Release 5.4 S O P.

Panini Scanners

Updates have been made to correct some known issues with the Panini scanners:

- ◆ In previous versions of the P O S, the Panini scanner was unable to scan additional checks once the hopper was empty and caused an error condition during batch processing mode. This issue has been corrected with Release 5.4.
- ◆ When the P O S computer went into a power save mode, the Panini scanner would lose the connection with the computer causing an error condition. With Release 5.4, whenever the computer goes into power save mode the user is logged out of the system.

Queue Interface (Currently for Military Agencies Only)

A new functionality called ‘Queue Interface’ enables a Military Agency’s DDS Application to interface with the PCC OTC application. Queue Interface accommodates a single transaction input for both the Agency and PCC OTC applications, and provides the ability to store information so both applications can share common transaction data.

During the Release 5.4 installation, users are prompted to install the Queue Interface with a ‘Yes’ or ‘No’ question.

Non military agencies would simply choose ‘No’. Military Agencies interested in using the Queue Interface

should respond with ‘Yes’.

Upon installation, a new permission called, ‘Configure Queue Interface’ is added, but it is not assigned to a role.

After installation is complete,

the P O C must sign on to the SAT and assign a role to the new ‘Configure Queue Interface’ role.

Complete information on the Queue Interface can be found in *Chapter 13, Queue Interface* of the Release 5.4 S O P.

Security Best Practices cont....

Incident Response

Monitor the PCC OTC system for possible security incidents and report any suspicious activity to the PCC OTC Customer Service staff.

System and Information Integrity

- Protect the P O S computer and its removable media against viruses, spyware and all other forms of malicious code.
- Use verification methods to ensure the accuracy of input.
- Include the use of the P O S Batch List feature, to verify batch transmission totals.
- Prevent duplicate processing of checks by electronically or hand stamping checks with the words ‘Electronically Processed/Presented’.

Questions?

If there are questions regarding any issues in this bulletin, please contact the PCC OTC Customer Service staff.

Federal Reserve Bank of Cleveland
PCC OTC Customer Service
PO Box 6387
Cleveland, OH 44101
Tel: 800-624-1373 or 216-579-2112
DSN: 510-428-6824, press 4, then 5, then 4
Fax: 216-579-2813
<https://www.pccotc.gov/pccotc/index.htm>