

MVD/CIRA Database Authorization Request

This form is completed by those individuals that are authorized to approve other individual's access to the MVD and CIRA. Please note that a person is not eligible to authorize him/herself.

Agency: _____

Eight Digit ALC or DSSN: _____

I hereby approve below, the following individual(s) as PCC Security Contact to submit user requests to MVD/CIRA on behalf of my agency site for Paper Check Conversion.

PCC Security Contact: _____

Signature

Date

Name & Title (printed or typed)

E-mail

Phone (Commercial and DNS Country Code)

PCC Security Contact: _____

Signature

Date

Name & Title (printed or typed)

E-mail

Phone (Commercial and DNS Country Code)

Approved by: _____

Supervisor / Manager Signature

Date

Name & Title (printed or typed)

E-mail

Phone (Commercial and DNS Country Code)

Return this form to: Federal Reserve Bank of Cleveland
P.O. Box 6387, Cleveland Ohio 44101-1387
Attn: Information Security Department
email:PCC@clev.frb.org
FAX: 216-579-3175

Paper Check Conversion
Master Verification Database /Central Image and Research Archive
Change Request

Agency: _____ **Eight Digit ALC or DSSN:** _____

Instructions:

Please specify the Paper Check Conversion (PCC) system for which this change is requested and then complete the form below as appropriate to the type of modification required. Please note, all changes must be approved by the senior officer or manager and then mailed to the Federal Reserve Bank of Cleveland.

PCC System: ___ Master Verification Database Or ___ Central Image and Research Archive
Or ___ Master Verification Database Reports Or ___ Central Image and Research Archive Reports

___ **ADD** ___ **PERSONNEL CHANGE FOR USERID:** _____

(List specific UserID)

The following party has been designated as a PCC user for this location. The individual listed below has agreed not to disclose his/her password to others, and has been advised that he/she is responsible for all actions related to the use of his/her ID within the PCC system. He/she also understands that unauthorized disclosure of any PCC information may be cause for loss of access and disciplinary action.

Name (printed or typed) Rank / Title

Signature

E-mail Phone (Commercial)

FAX Phone (DSN Country Code)

Address (Country and APO if applicable) City / State Country / Zip

MVD Role: ___View ___Edit

Sites to be Viewed (Central Image and Research Archive users)

Access will remain in effect until notice is provided to the Federal Reserve Bank of Cleveland.

DELETE:

UserID: _____ Name: _____
(printed or typed)

Approved by: _____
PCC Security Contact Date

Name & Title (printed or typed)

E-mail Phone (Commercial and DNS Country Code)

FEDERAL RESERVE BANK OF CLEVELAND USER RESPONSIBILITY STATEMENT

LOGON ID AND PASSWORD:

The Federal Reserve Bank (FRB) of Cleveland will e-mail the individual logon ID and user must call in for temporary password. The password, which is under your sole control, provides protection for you and us. The pattern of your logon ID may be known by others and the logon ID is displayed on the screen when entered, but your password is not displayed and not known by anyone other than you. After initial logon, all Paper Check Conversion (PCC) system users must access the system at least once every ninety - (90) day's to remain active. After ninety - (90) days of non-use, your logon ID is deactivated and new paperwork must be submitted to FRB Cleveland to reissue your ID. If at any time during the log-on process, the individual's logon ID or password should become suspended please contact the FRB Customer Support.

USER RESPONSIBILITIES:

Once assigned a logon ID and Temporary password by the FRB of Cleveland, you agree to be responsible for the consequences that result from the disclosure or use of your password. To avoid compromising your password, you agree that you will:

- Not make your password known to anyone or put it in written form unsecured.
- Prevent others from watching you enter your password and guessing your password (for example, you should not use names of persons, places, or things that are identified with you).
- Log off of the system whenever you leave your computer unattended.

Your password expires after 30 calendar days and the system will automatically prompt you to reset password. If you feel that your password has been compromised, it must be changed immediately. In addition, you must report unauthorized use to FRB Customer Support.

U.S. Treasury Department – Financial Management Services Paper Check Conversion (PCC) System IT Security RULES OF BEHAVIOR

Please read the following rules and sign.

Users must ensure that the information technology (IT) resources with which they have been entrusted are used properly, as directed by FMS policies and standards, taking care that the laws, regulations, and policies governing the use of such resources are followed and that the value of all information assets are preserved. Each user is responsible for all activities associated with their assigned User ID.

Users must follow approved FRB procedures to request or to revoke access to the PCC system. Users must complete and submit the appropriate access change request forms. Forms are available on the FMS PCC Web page (www.pcc.gov).

Users must take positive steps to protect FMS equipment and, systems, software, and data from loss, theft, damage, and unauthorized use or disclosure. Users must report improper or suspicious use of FMS equipment and systems to the FRB Customer Support.

Users must ensure that unauthorized individuals cannot view screen contents.

Users must protect User IDs and passwords from improper disclosure. Passwords provide access to FMS any agency data and resources. Users are responsible for any access made under his/her User ID and password.

Users:

- Do not reveal passwords under any circumstances. Password disclosure is considered a security violation and is to be reported as such. If password disclosure is necessary for problem resolution, immediately select a new password once the problem has been resolved.
- Do not share passwords with anyone else or use another person's password.
- Do not write passwords down, unless secured.
- Must change passwords at least every 30 days.
- Must choose hard to guess passwords, using a minimum of eight case-sensitive alphanumeric and/or special characters. Example: Pass\$word.

Users must not attempt to circumvent any PCC system security control mechanisms.

Users must follow proper logon/logoff procedures. User is aware that his/her assigned User ID and password serve as his/her electronic signature, therefore, accepting responsibility, for all activity while active in the PCC system.

Users must utilize anti-virus protection mechanism(s) on any systems connecting to FMS applications.

Users must complete and document IT security awareness, training and education as required by applicable government directives.

Users must report any known or suspected breaches of PCC system security to the FRB Customer Support immediately after discovery of the occurrence.

ACCEPTANCE

Please acknowledge acceptance of the User responsibilities and the IT Security Rules of Behavior by signing below.

I have read the Federal Reserve Bank of Cleveland's User Responsibility Statement, agree to its terms, and understand my responsibilities for the use and protection of my logon ID and password. Further, I understand the consequences that may result from disclosure or inappropriate use. If I fail to adhere to any of the terms in this statement, the Federal Reserve Bank of Cleveland may revoke my logon ID and take other appropriate action.

AND

I have read the Financial Management Service (FMS) IT Security Rules of Behavior for the PCC system and fully understand the security requirements of the information systems, applications and data. I further understand that violation of these rules may be grounds for revocation of my User ID and may result in actions up to and including prosecution under federal law.

User's Name (printed): _____ Date

User (Signature): _____

Return this form to:

Federal Reserve Bank of Cleveland
Attention: Information Security Department
1455 East Sixth St., Cleveland Ohio 44114
Email: PCC.Security@clev.frb.org
FAX: 216.579.3175

For PCC Support:

800.624.1373
216.579.2112
fax: 216.579.2813
email:PCC@clev.frb.org