Treasury Check Information System (TCIS)

Internal Enrollment Request Form

Please type or legibly print information

Action Requested:
(Check One Box)

- ❑ New Request
- ❑ Modify
- ❑ Revoke

User Name: _____ _____ _____
(Full Legal Name) First Name M. I. Last Name

Agency Name: _____

Bureau Name: _____

AC Area: _____

Branch: _____

Street address including room number *(PO Box is not acceptable)*:

Street *(Line1)*: _____

Street *(Line2)*: _____ **Room No.:** _____

City: _____ **State:** _____ **Zip Code:** _____

User Work Email Address: _____

User Work Phone Number: (_____) _____

User Signature: _____ **Date:** _____

Supervisor Name: _____

Supervisor Title: _____

Supervisor Work Email Address: _____

Supervisor Work Phone: (_____) _____

Supervisor Signature: _____ **Date:** _____

Please type information onto form, print, provide signatures, then

Fax to: TCIS Support Center
866-707-6574

or

Mail to: TCIS Support Center
Federal Reserve Bank of St. Louis
1421 Dr. Martin Luther King Drive
St. Louis, MO 63106-3716.

Send Questions to: TCIS_TSC@stls.frb.org
Customer Service: 855-838-0743 or 314-444-6151

TCIS Modules:

Integrated View (IV) – Provides a single access point to the TCIS, and PACER databases to query and view check and ACH data and view images of paid checks. Access roles to this module are indicated by IV in the roles. Access roles with IV-UCC additionally provide the ability to submit a stop code against a particular check symbol/serial number.

Transmittal Control and Disbursing Office Maintenance Subsystem (TCDOMS) –
Provides Disbursing Offices on-line access to monitor and track the status of transmittals that they have submitted, providing a complete history of each transmittal received and detail information concerning rejected transmittals. Users can view all authorized ranges established for their Disbursing Office Symbol and display all issue transmittals received and accepted by TCIS for a particular authorized range by viewing the Processed Ranges screen.

Please identify your Organization Type and select only **one** TCIS role included under the Organization Type. List either the Agency Location Codes or the Disbursing Office Symbol numbers that you require access to on the line provided. If additional space is required, continue on a blank sheet and indicate (continued) on the line provided.

Treasury Disbursing Office (TDO) Roles

- ❑ TDO–IV
- ❑ TDO–TCDOM
- ❑ TDO–TCDOM–IV
- ❑ Dashboard

TDO – May inquire and view images on all checks in IV and inquire on check symbols, check ranges and transmittals used by Treasury Disbursing Offices in TCDOMS.

Federal Program Agency (FPA) Roles

- ❑ FPA–Agency–IV
- ❑ FPA–Agency–IV–UCC

FPA – May inquire and view check images for one or more 8-digit Agency Location Codes in IV. Roles with UCC indicate additional ability to submit a stop code against a particular check symbol/serial number. FPAs are not permitted access to TCDOMS.

List Agency Location Codes: _____

_____

_____

_____

_____

_____

For Payment Management Employees Only

Please check the requested application and roles:

	INTEGRATED VIEW AND TC DOMS	DMI	FRONTIER	PEGA	STORER	DASHBOARD
OD (Office of the Director)	❑ FMS-CRD Director	❑ FMS-CRD Director ❑ Security Administrator	❑ FMS-CRD Director ❑ Security Administrator	❑ FMS-CRD Director ❑ Security Administrator	❑ FMS-CRD Director ❑ Security Administrator	❑ CRD Manager ❑ ISSO Admin
QDS (Questioned Documents Staff)	❑ FMS-QDS	❑ Scanner/ Profiler*	❑ Lead ❑ Analyst	❑ Lead ❑ Analyst	❑ Lead ❑ Analyst	❑ QDS Lead ❑ QDS User
AB (Accounts Branch)	❑ FMS Accounts Branch ***(NO ACCESS TO TCDOMS)***	❑	❑ AB	❑	❑ AB-ALL	❑ AB Supervisor ❑ AB User ❑ AB Adjustment
CCB (Check Claims Branch)	❑ FMS Claims ❑ FMS Claims UCC ❑ FMS Claims ODM	❑ Scanner/ Profiler*		❑ Manager ❑ Supervisor ❑ Lead ❑ Specialist ❑ LAS ❑ Clerk ❑ Clerk Assistant ❑ Clerk Holder & Due Course	❑ Manager ❑ Supervisor ❑ CCB-ALL	❑ CRD Manager ❑ CCB Supervisor ❑ CCB User
CRB (Check Reconciliation Branch)	❑ FMS Recon Manager ❑ FMS Recon Technician	❑ Scanner/ Profiler*	❑ Manager ❑ Technician	❑	❑ Manager ❑ CRB-All	❑ CRD Manager ❑ CRB User
RB (Reclamation Branch)	❑ FMS Reclamation ***(NO ACCESS TO TCDOMS)***	❑ Scanner/ Profiler*		❑ Manager ❑ Lead Collection Specialist ❑ Collection Specialist ❑ Collection Technician ❑ Administrative Assistant	❑ Manager ❑ Lead Collection Specialist ❑ RB-ALL	❑ RB Manager ❑ RB Supervisor ❑ RB User
FRB	❑ FRB CBAF	❑ FRB CBAF	❑ FRB CBAF	❑ FRB CBAF	❑ FRB CBAF	❑ CBAF User

**Requires VPN Access - please complete VPN Access Request form and VPN ROB located on the TCIS website.*

BFS GENERAL SUPPORT SYSTEM SECURITY RULES OF BEHAVIOR

- USERS must ensure that the information technology (IT) resources with which they have been entrusted are used properly, as directed by BFS 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 be knowledgeable about BFS IT policies and standards. As systems change, USERS are required to seek additional information in order to ensure current policies and procedures are followed.
- USERS must take positive steps to protect BFS equipment, software, and data from loss, theft, damage, and unauthorized use or disclosure.
- USERS must report improper or suspicious use of BFS equipment.
- USERS must not attempt to circumvent any BFS IT security control mechanisms.
- USERS must follow proper logon/logoff procedures.
- USERS must use the BFS provided virus protection mechanisms as intended.
- USERS must protect digital media from extreme temperatures, bending, fluids, smoke, etc. and in addition, protect magnetic digital media from magnetic fields.
- USERS will ensure that media is secured based on the sensitivity of the information contained, practicing proper labeling procedures.
- USERS must complete and document IT security awareness, training and education as required by BFS policies and standards.
- USERS must not read, alter, insert, copy, or delete any BFS data except in accordance with assigned job responsibilities. Ability to access data does not equate to authority to manipulate data. In particular,
- USERS must not browse or search BFS data except in the performance of authorized duties.
- USERS must not reveal information produced by the BFS IS except as required by job function and within established procedures.
- USERS must protect BFS communications/connectivity integrity. Dial-in or other remote access to BFS is prohibited, unless specifically authorized.
- USERS must comply with and provide assistance with IT audits and reviews as appropriate.
- USERS must report any known or suspected breaches of IT security to IT management immediately after discovery of the occurrence.
- USERS must not install or use unauthorized software on BFS equipment. Do not use freeware, shareware, or public domain software on BFS computers without your supervisor's written permission and without scanning for viruses.
- USERS must observe all software licensing agreements. Do not violate federal copyright laws.
- USERS must retrieve all hard copy printouts in a timely manner.
- USERS must complete background investigation materials by due date.
- USERS must ensure that anyone seen using a BFS workstation in the area is authorized to do so. This includes challenging unauthorized visitors. When leaving an active BFS workstation unattended, users will log off or secure the workstation from unauthorized use.
- USERS will facilitate and participate in IT system service restoration after a disruption.

➢ USERS must protect user IDs and passwords from improper disclosure. Passwords provide access to BFS data and resources. USERS are responsible for any access made under his or 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 program login IDs or passwords into automatic script routines or programs.
- Do not share passwords with anyone else or use another person's password.
- Do not write passwords down.
- Change passwords at least every 90 days.
- Choose hard to guess passwords, using a minimum of eight alphanumeric and/or special characters.

Users shall report any suspected loss or compromise of private keys for a system using Public Key Infrastructure security to the incident response team.

ACCEPTANCE

I have read the Bureau of the Fiscal Service (BFS) information technology Rules of Behavior and fully understand the security requirements. I further understand that violation of these rules may be grounds for administrative and/or disciplinary action by the BFS and may result in actions up to and including termination or prosecution under federal law.

_____ _____

User Name *(Please print)* Date *(MM/DD/YYYY)*

_____

User Signature