Bureau of Indian Education and Office of the Special Trustee

FEDERAL PERSONNEL/PAYROLL SYSTEM (FPPS)

USER ACCESS REQUEST (UAR) FORM

By signing this form, I understand that when I use any of the Interior Business Center (IBC) Computer Systems and/or Automated Information Resources or gain access to any information therein, such use or access shall be limited to official Government business. Further, I understand that any use of the aforementioned systems or information that is not official Government business may result in disciplinary action consistent with the nature and scope of such activity. I have read the attached FPPS user access request form information and the Rules of Behavior. I understand them and I agree to comply with them. **I WILL REPORT ANY VIOLATION OF THESE RULES TO MY SUPERVISOR**. Any references made to the Agency should be regarded as being inclusive of the Assistant Secretary – Indian Affairs (AS-IA), Bureau of Indian Affairs (BIA) and Bureau of Indian Education (BIE) personnel who use FPPS or perform administrative and security related duties in its operation. This form supersedes previously submitted forms.

Action Request: ☐ New User ☐ Recertify ☐ Reactivate ☐ Change/Update ☐ Delete User

Employee Type: ☐ Permanent ☐ Temporary ☐ Contractor ☐ Other _____

Organization: ☐ BIE ☐ OST

FPPS: USER INFORMATION **(Type or Print when Competing Form)**

_____ FPPS User ID: _____

Last, First MI (Legal)

*SSN (Last 4-Digits): XXX-XX- _____ Employee's Organization Code: _____

Telephone Number: _____ _____

Duty Location (City & State)

_____ _____

Employee Work Email Address Supervisor/Manger Name & Title

User Access Special Instruction:

FPPS: AUTHORITIES USER REQUESTING

☐ Initiator (INI) ☐ Requestor (RA5) ☐ Authorizer (RA6) ☐ Concurrer (CC1)

☐ View Only ☐ SPO User ☐ SPOC Admin

FPPS: ORGANIZATION CODE RANGE

WTTS: TYPE OF ACCESS (if applicable)

☐ Supervisor ☐ HR Rep ☐ EEO ☐ View Only ☐ Security Admin

_____ _____ _____ _____

Employee Signature Date Supervisor/Manager Signature Date

Return form to the HR Systems FPPS-WTTS Security Administrator

Primary: Anna Smith Desk: (405) 247-8023 Fax: (405) 247-8010 email: anna.smith@bia.gov

Alternate: Jacqueline Benavides Desk: (505) 563-5313 Fax: (505) 563-5305 email: jacqueline.benavides@bia.gov

FOR SPOC USE ONLY

Form Rec'd: _____ DSAF Subm: _____ DSAF Rtd: _____ FPPS User ID: _____

USER: _____ RPTH: _____ WGI/PRB RPTH: _____ User Notified: _____

Processed By: _____ Remarks: _____

*Privacy Act Statement: Solicitation of your Social Security Number (SSN) is authorized by Executive Order 9397, which requires agencies to use the SSN as the means for identifying individuals in personnel information systems. Your SSN will only be used to establish your access to the HR System requested. Furnishing your SSN is voluntary and failure to do so will have no effect on you. However, where individuals decline to furnish their SSN, the SSN will be obtained from other records in order to process the request for access.

FPPS-WTTS USER ACCESS REQUEST FORM INFORMATION:
(DO NOT submit with form – Retain with your records)

FPPS Authorities/Roles:

- Initiator (INI): A requesting office user who can create/initiate SF-52 transactions. Has no signature authority.
- Requestor (RA5): A requesting office user who can create/initiate SF-52 transactions and has a requester signature authority.
- Authorizer (RA6): A requesting office user who has SF-52 authorizer signature authority. This approval signature is required on all actions.
- Concurrer (CC1): A user who has SF-52 concurrence signature authority. This access is usually a budget person.
- View Only: Has viewer capability only. This command is automatically granted with other FPPS roles.
- SPO User: A servicing personnel office user.
- Security Point of Contact (SPOC) Admin: A limited number of HR employees who establish and maintain FPPS users.

FPPS: Org Code Range: List the entire range of organizational codes the user needs to be able to access (i.e. P00101-P18999)

System Access Revocation:

Password expiration. If a new user account is created or an account password is reset and the user never signs on, they will be revoked after 24 hours.

User Inactivity. If a user was active at some date and then is inactive for more than 45 days, they will be revoked.

Invalid Attempts. A user will be revoked after 3 invalid password attempts.

FPPS-Admin Revocation. A user will be revoked for unauthorized use or disclosure or failure to comply with policy or other program requirements. Supervisors or higher level authorities can also request user's accesses be revoked. Unauthorized use may subject users to criminal, civil, and/or disciplinary action.

All users who lapse into a revoked status for 6 months or more will be required to submit a new FPPS User Access Request Form.

After 12 months of being in a revoked status, users will be inactivated completely by the Denver IBC IT Services Office.

System Access Removals:

The removal of a user's access to the IBC mainframe system and FPPS is based on a person's departure from Agency for any reason, non-use of accesses, transfers within the Bureau to other Regions or ERC, changes in duties or requests by proper authority to have a user's accesses removed. Access removals may also include departure due to resignation, death, retirement or medical leave of absence. To assist in ensuring terminations are processed timely, the Security-Admin will pull regular separation and position change reports.

RULES OF BEHAVIOR FOR USERS OF
COMPUTER SYSTEMS AND APPLICATIONS HOSTED AND MANAGED BY
DEPARTMENT OF THE INTERIOR, INTERIOR BUSINESS CENTER
(DO NOT submit with form – Retain with your records)

The following Rules of Behavior (ROB) apply to all users of FPPS and must be reviewed by all users before granting them access to the Federal Personnel Payroll System (FPPS).

1. **User Identification:**
   - A unique User ID is required for each individual FPPS user.
   - User IDs must never be shared between users. o User IDs possess privileges that are tailored to the duties of the individual user's job and to the individual user's level of "need-to-know." Each change in access must be made in writing using the attached form and approved by the user's supervisor. Completed forms are forwarded to the Office of Human Resources Systems Security-Admin personnel (see attached form).
   - If duties or job requirements change, accesses no longer needed must be removed and new accesses must be requested. Supervisors are responsible for notifying the Security-Admin personnel whenever such changes occur so that the user's accesses can be changed to suit the new duty or job requirements.
   - When employment terminates, for any reason, a user's access must be terminated. Supervisors are responsible for notifying the Security-Admin personnel whenever a user leaves the organization, so that the user's access authorities can be removed. Under no circumstances may the logon account of a terminated user be given to another individual.

2. **Passwords:**
   - Passwords are considered private and confidential. Users are prohibited from sharing their FPPS password(s). Attempting to enter an incorrect password three times will result in your user access being revoked. If you receive a message stating that you have been revoked, contact one of the SPOCs.
   - To minimize the risk of having the system compromised as a result of poor password selection; users are responsible for selecting passwords that are difficult to guess. FPPS users must follow these password guidelines:
     - Passwords must be eight characters exactly – no more, no less.
     - Passwords must begin and end with an alpha-character.
     - Passwords must contain at least one numeric character in positions 2 through 7.
     - New (changed) passwords may not be revisions of an old password. Reuse of the same password with a different prefix or suffix is not permitted.
     - Dictionary words, derivatives of User IDs, and common character sequences may not be used.
     - Personal details such as a spouse's name, license plates, social security numbers and birthdays should not be used unless accompanied by additional unrelated characters.
     - Proper names, geographical locations, common acronyms, and slang should not be used.
     - If exposed or compromised, passwords must be changed immediately.

3. **General User Responsibilities**
   - Users are responsible for using IBC-managed computer systems and associated data for business purposes only.
   - Users of IBC-managed systems and applications may not access, or attempt to access, data for which they are not authorized.
   - Users are responsible for protecting the confidentiality of data associated with the IBC-managed system or application to which they have been granted access, based on the sensitivity of the data. Such data may not be given to unauthorized persons.
   - Users should report suspected or actual security violations to their supervisor or Security-Admin/SPOC, and where appropriate, to the application security administrator.

- Casual browsing of sensitive or Privacy Act FPPS information, such as personnel data, is prohibited. FPPS users should only access FPPS data when there is an official business reason.
- Users are accountable for all actions associated with the use of their assigned user ID and may be held responsible for unauthorized actions found to be intentional, malicious, or negligent. Each user must protect his/her user ID by never allowing another person to use or share his/her logon session. Because the logon session is directly associated with an individual user ID, the user is personally accountable for all actions performed with the user ID.
- When employment terminates, for any reason, a user's access must be terminated. Supervisors are responsible for notifying the Security-Admin personnel whenever a user leaves the organization, so that the user's access authorities can be removed. Under no circumstances may the logon account of a terminated user be given to another individual.

4. Security-Admin/Point of Contact

Security-Admin/SPOCs are designated for each organization. Access to production data is approved and controlled by the data owner, through the SPOC for each application or system. SPOCs are responsible for:

- Approving and coordinating all requests for user access to the systems or applications they control.
- Complying with the ROB, which is completed during the SPOC assignment process and returned to the IBC IT Security Administration Office.
- Implementing controls to provide reasonable assurance that:
  - Physical and logical access to IBC-managed systems and applications, using computer terminals, is restricted to authorized users.
  - Audit reports of system use, made available by the IBC, are regularly reviewed.
  - Computer Security Incident Response procedures are in use at the user's site for reporting incidents involving or impacting IBC-managed systems and applications.
  - User access to IBC-managed systems and applications is properly authorized and assigned, and that segregation of duties is properly maintained.
  - Reporting all suspected or actual security violations involving an IBC-managed system or application, to the IBC IT Security Administration Office.

5. Consequences for Non-Compliance with these Rules of Behavior

The consequences of Federal employee or contractor behavior not consistent with these rules may result in revocation of access to FPPS, and wherever such actions may be applicable, disciplinary action consistent with the nature and scope of the infraction may be applies