CORPORATE SYSTEMS ACCESS REQUEST FORM
SECURITY RULES

VIOLATION OF THESE RULES
MAY RESULT IN
DISCIPLINARY ACTION

1. **DO NOT ACCESS**, research, or change any account, file, record or application not required to perform your official duties. You are forbidden to Access your own account, that of a spouse, relative, friend, neighbor, or any account in which you have a personal or financial interest. If you are assigned to work on one of these accounts contact your supervisor. Behave in an ethical, technically proficient, informed, and trustworthy manner.

2. If you are asked by another person to access an account or other sensitive or private information, **VERIFY** that the requested access is authorized. You will be held responsible if the access is not authorized. As a general rule, you should not use a computer or terminal in behalf of another person.

3. **DIFFERENTIATE TASKS AND FUNCTIONS** to ensure that no one person has sole access to or control over important resources.

4. **PROTECT YOUR PASSWORD** from disclosure. You are responsible for any computer activity associated with your password**. DO NOT SHARE** your password with others or reveal it to anyone, regardless of his/her position in or outside the USDA. **DO NOT POST** your password in your work area. **DO NOT USE** another person’s password. USER Ids must be treated with the same care as your password. Everything done with your user ID or password will be recorded as being done by you. Use unique passwords for each system and application you access. NEVER give your password out over the telephone. Be alert to others who may try to obtain your password. Social engineering is a practice used when hackers pose as system administrators. A hacker may randomly call a user and say that something is wrong on the system to get arbitrary access to your system. They may tell you that they need your password in order to issue an new one. Always remember that system administrators DO NOT need your password in order to issue you a new password. Do not re-cycle passwords by using just a few over and over again, or make minor changes to passwords by adding a number to the base password.

5. **PASSWORD DISTRIBUTION AND REFRESHMENT** must be done securely.

6. **CHANGE YOUR PASSWORD** if you think someone else knows your password. Immediately notify your supervisor or your Functional Security Coordinator or Security Representative. Passwords for FFIS, IAS and the FFIS Data Warehouse will be changed every 30 days as prompted by the system.

7. **DO NOT PROGRAM** your login or password into automatic script routines or programs.

8. **LOG OFF/SIGN OFF** if you go to lunch, or break, or anytime you leave your computer or terminal.

9. **PROTECT** your system against viruses and similar malicious programs. Make certain that updates to desktop virus protection schemes are performed in a timely manner in accordance with vendor or system administration instructions.

10. **FOR ADDITIONAL** security, use personnel firewall applications and do not allow applications not known to you through the firewall.

11. **PARTICIPATE** in organization-wide security training as required and read and adhere to security information pertaining to system hardware and software.

12. **RETRIEVE ALL** hard copy printouts in a timely manner. If you cannot determine the originator or receiver of a printout, dispose of it in a burn waste container or shredder. Store all hardcopy reports and storage media containing Confidential information in a locked room or cabinet.

13. **IDENTIFY ALL** sensitive applications or data that you will be placing on a system, and any equipment processing sensitive information to your Supervisor, so that appropriate security measures can be implemented.

14. **DO NOT USE USDA COMPUTERS** or software for personal use.

15. **DO NOT USE PERSONAL EQUIPMENT** or software for official business without your supervisor’s written approval.

16. **DO NOT INSTALL OR USE UNAUTHORIZED SOFTWARE** on USDA equipment. Do not use freeware, shareware or public domain software on USDA computers without your supervisor’s permission and without scanning it for viruses. Comply with local office policy on the use of antiviral Software.

17. **OBSERVE ALL SOFTWARE LICENSE AGREEMENTS.** Do not violate Federal copyright laws.

18. **DO NOT MOVE EQUIPMENT** or exchange system components without authorization by the appropriate functions and manager’s approval.

19. **PROTECT USDA COMPUTER EQUIPMENT** from hazards such as liquids, food, smoke, staples, paper clips, etc.

20. **PROTECT MAGNETIC MEDIA** from exposure to electrical currents, extreme temperatures, bending, fluids, smoke, etc. Ensure the magnetic media is secured based on the sensitivity of the information contained, and practice proper labeling procedures. **BACK UP** critical programs and data, and store in a safe place. Back ups should be performed as often as program and data sensitivity require. Erase sensitive data on storage media before reusing or disposing of the media.

21**.** **DO NOT DISCLOSE THE TELEPHONE NUMBER(S)** or procedure(s) which permit system access from a remote location.

22. **DO NOT SEND OR STORE** Government information on a commercial E-mail site.

23. **DO NOT USE** sensitive information for equipment or program test purposes. Vendors should be escorted and monitored while performing maintenance duties.

24. **DO NOT DISCLOSE** or discuss any USDA personnel or vendor related information with unauthorized individuals. The Privacy Act of 1974, 5 USC 552a, prohibits such disclosure. A person making a willful unauthorized disclosure of information covered by this act may be charged with a Misdemeanor and subject to a fine of up to $5,000.

25. **PROMPTLY REPORT** all security incidents to your supervisor and in accordance with you agency policy on reporting incidents. For example: unauthorized disclosure of information, computer viruses, theft of equipment, software or information, and deliberate alteration or destruction of data or equipment. NEVER assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident is reported more than once.

26. **SEEK** assistance and challenge unescorted strangers in areas where the system is being used.

27. **Complete this form when Duties Change, when a separation from the agency occurs, and to report name changes or request profile changes.**

AD-1143 FORM INSTRUCTIONS

BLOCK NO.

1 Check one or more systems. Fill in information for access in Special Instructions for FedTraveler.com

2 Enter the agency FFIS application number, i.e., FF34 for APHIS, or FF11 for Forest Service.

USER INFORMATION

3 Enter social security number. **The Social Security Number is only required for adding a user to a FFIS application for the first time.**

4 Enter name.

5 Enter job title or Contractor, if not a USDA employee.

6 Enter address where the user can be contacted by mail.

7 Enter agency name and agency code/number.

8 Enter office, i.e., Financial Management, Procurement Operations.

9 Enter e-mail address.

10 Enter telephone number.

11 Enter manager's telephone number.

ACTION REQUESTED

12 Enter "old" name, when requesting a name change.

13 Enter "new" name, when requesting a name change.

14 Check the appropriate action to be taken. If requesting a modification to your profile, specify in Block 29 the previous profile or job assignment and the new profile or job assignment. If the user performs services for additional USDA agencies, e.g., "cross-servicing, specify the additional agencies(s) and required roles.

15 Enter NFC, FFIS, E-Auth, and AgLearn userids AND if Block 14 is "delete user" or "modify user", include existing userid. If action requested in Block 14 is "add user", the Agency Security Administrator will assign the userid.

AUTOMATED CASH RECONCILIATION WORKSHEET SYSTEM ACCESS

16 Check appropriate Role(s)/Access for ACRWS52.

17 Check appropriate Role(s)/Access for ACRWS53.

18 Reserved.

CORPORATE PROPERTY AUTOMATED INFORMATION SYSTEM ACCESS

19 Check the appropriate action to be taken. If requesting a modification of your user CPAIS role, specify all role(s) deleted and/or added.

21 If requesting UMA manager, this must be approved at a department level.

FINANCIAL DATA WAREHOUSE SYSTEM ACCESS

22 Check the appropriate box to grant level of access. Security group is for Security Administrators or individuals who need access per job duties.

23 Check the appropriate box to grant level of report access. Check only one box.

FINANCIAL MANAGEMENT MODERNIZATION INITIATIVE ACCESS (FMMI)

24 Check applicable User Role Set or enter a name of an existing user as Look Alike for setup purposes. Follow the directions given for obtaining the correct AgLearn userid and name as listed in your eAuth profile.

INTEGRATED ACQUISITION SYSTEM ACCESS

25 Check all appropriate roles.

26 Enter requisition approval amount, if user is a Funds Approver.

27 Enter warrant amount, if user is a Contracting Officer. Verify the amount to be entered here with your supervisor if you are warranted for a higher amount than your supervisor has authorized you for.

28 Does this user purchase for other agencies? If yes, enter the agencies here, e.g., Rural Development, Food and Nutrition Service.

MANAGEMENT INITIATIVES TRACKING SYSTEM ACCESS

26 Check required role.

See USDA Corporate Website or the MITS Security Features User's Guide for definitions of each role. Only one role per MITS module should be entered on an individual AD-1143; complete separate AD-1143 documents for each additional role.

For PMA: Enter appropriate initiative(s).

HC – Human Capital
RP – Real Property
FM – Financial Management
FBCI – Faith Based
IPIA – Improper Payments
CS – Competitive Sourcing
CP – Credit Programs
eGov – Egovernement
R&D – Research and Development
BPI – Budget and Performance Integration

Enter appropriate agency(s).

For PART: Enter appropriate program(s) or "ALL", default is "ALL".
Enter appropriate agency(s).
Enter mission area(s) (required for mission area coordinators only).
Enter PART program(s) – optional (enter if user should have edit access for limited PARTs)

For BUDGET: Enter appropriate agency(s).

For AUDIT TRACKING: Enter appropriate agency(s).
Enter mission area(s) (required for mission area coordinators only).
Executive Officer and OIG Auditors role – Available to OCFO employees and OIG auditors only.
Audit Follow-up Coordinator role – Available to OCFO employees only.

For Sustainability Scorecard: Enter appropriate initiative(s).
Enter appropriate agency(s).

GOVTRIP.COM

27 Please check the role the user will be in GovTrip.

Traveler – Only view their travel data and submit their own voucher for approval.
Travel Arranger – Able to prepare travel plans for designated personnel in their agency's organization and able to see the information of others.
Approver—Able to approve travel vouchers for designated personnel in their agency's organization.
Agency FATA – Able to set up configuration for their designated agency. This should be only a few personnel.

28 Indicate if training has been received.

29 Signature of the requester's supervisor or designated travel manager in the agency.

SPECIAL INSTRUCTIONS

30 Include any additional information needed to complete access. Specify the security profile or job assignment, or any comments or special instructions.

For CPAIS: Provide organization number(s) for which access is being requested. If access is needed for all organizations within an agency, list agency name and "ALL".

For FFIS/FMMI 1) Provide previous profile or job assignment and the new profile or job assignment, if modification to existing model; and
2) Provide the names of the additional agencies(s) and required roles, if the user performs services for additional USDA agencies, e.g., "cross-servicing".

USER ACKNOWLEDGEMENT

A USER SIGNATURE IS REQUIRED IN THE USER ACKNOWLEDGMENT BLOCK WHEN THEY ARE ADDED TO A SYSTEM.

31 User's signature.
32 Date user signed form.

BACKGROUND INVESTIGATION

THIS FIELD MUST BE FILLED OUT. SECURITY ADMINISTRATORS WILL NOT COMPLETE THE REQUEST UNLESS THIS BOX IS FILLED OUT ACCORDING TO THE INSTRUCTIONS BELOW

33 Check whether background investigation has been initiated or completed. This applies to both USDA employees and contractors.
34 Date background investigation was initiated or completed.
35 Name of user's immediate manager

AUTHORIZATION

36 Manager's signature.
37 Date manager approved the requested action.

ACTION TAKEN

38 Security Administrator's signature.
39 Date Security Administrator completed user's request.
40 Security Administrator can use this space to include any notes related to the completion of the request. The agency's Security Administrator will retain each completed form for audit purposes.