Print

OMB APPROVED NO. 0584-0532
Expiration Date: XX/XX/XXX

U.S. Department of Agriculture - Food, Nutrition and Consumer Services

User Access Request Form

User Information

1. Last Name	First Name	Middle Name	2. Title	3. Date of Request

4. Work Email	5. USDA E-Auth User ID, *(if applicable)*

6. Type of User *(select one)*	7. Telephone	8. Contract Expiration Date *(if applicable)*	9. Temporary Employee Expiration Date *(if applicable)*

10. Company/Agency	11. Functional Area	12. Division/Branch

13. Physical Duty Location *(select one)* **Physical Duty Street Address** **Suite/Unit #**

City **State** **ZIP Code**

14. System Name	15. Type of Access/Role	16. Action Requested

17. System Login User ID *(current users)*	18. Program and Form *(applicable for FPRS)*

19. State/Locality Codes

20. Comments or Special Instruction and/or Justification (if "Other" is selected in fields 6 or 13). *(attach separate sheet if more space is needed)*

Privacy Act Statement

The following information is provided in accordance with 5 U.S.C. § 552a(e)(3) and M-03-22.

Authority: This information is being collected under the authority of **5 U.S.C § 301**, **44 U.S.C. § 3101**, **Public Law 107-347**, and **Executive Order 13231**.

Purpose: This information is collected to ensure accounts are created with the correct information and access permissions for individuals.

Routine Uses: The information will be used to create accounts and grant access permissions. Additional disclosures are outlined in Office of Management and Budget (historical) **Circular A-108 in F.R. Vol. 40, No. 132 at 28949**, **Circular A-108 Reissuance**, and in greater detail with commentary on the Department of Justice **OVERVIEW OF THE PRIVACY ACT OF 1974** website.

Disclosure: Disclosing the information is voluntary. Failure to provide correct information will result in denial of account or access permissions.

The System of Records Notice for this information collection is under development in the USDA Office of the Chief Information Officer.

21. User Acknowledgement *(Users requesting system access must read, sign and date prior to submitting this form)*

- I have read and understand the Privacy Act Statement above and the FNCS Rules of Behavior on pages 3-4.
- Decisions in personnel matters involving disciplinary action will be based on the assumption that I am familiar with the security requirements presented in these rules and I am aware of my obligation to abide by them.
- I understand that systems require security to protect user and system files from unauthorized access.
- I have completed this form to the best of my abilities.

User Signature **Print Name** **Date**

Approvals

22. a. Supervisor/COR

Print Name ☐ Approve ☐ Deny

Phone Number Date Signature

b. System - Account Manager (FNCS)

Print Name ☐ Approve ☐ Deny

Phone Number Date Signature

c. State Computer Security Officer *(if applicable)*

Print Name ☐ Approve ☐ Deny

Phone Number Date Signature

Rules of Behavior *(ROB)*

Purpose

What are Rules of Behavior?

Rules of Behavior (ROB) describe user responsibilities and certain expectations of behavior in regard to accessing and protecting USDA and FNCS systems and data. In addition, rules of behavior outline the consequences of non-compliance and/or violations of the ROB. OMB Circular A-130, as well as USDA and FNCS policy, require that users acknowledge these rules of behavior before being granted access to agency systems and annually thereafter.

FNCS employees, contractors, and others granted access to the USDA internal IT network are required to comply with the Rules of Behavior for Internal Users. If FNCS/USDA provisions accounts for agency systems to external users (see below) through USDA eAuthentication Level 2 access, it is FNCS' responsibility to ensure that whomever the account is provisioned to reviews and accepts the Rules of Behavior for External Users.

Rules of behavior are updated periodically to reflect changes to Federal and USDA/FNS requirements. Users are required to re-sign the updated rules of behavior to affirm their understanding of the updated requirements.

Audience

Who is covered by the Rules of Behavior?

- **Internal Users**: Includes employees, contractors, affiliates, interns, volunteers, and fellows who work for, or on behalf of, FNCS/USDA. These individuals are issued a USDA Personal Identity Verification (PIV) credential and are provisioned access to the internal USDA IT network.
- **External Users**: Non-employees who have access to FNCS/USDA information systems, but who are not issued a USDA PIV credential or access to the USDA internal IT network. External users include customers and partners of FNCS/USDA.

Monitoring and Penalties for Non-Compliance

What are the consequences for violating the Rules of Behavior?

At any time, USDA and FNCS may monitor and/or audit user activity and/or network traffic. In addition, USDA may access the system and disclose information obtained through audits to third parties, including law enforcement authorities. Acceptance of the warning banner prior to logging into the FNCS network is your acknowledgment of the USDA and FNCS monitoring/auditing.

Compliance with these rules will be enforced through sanctions commensurate with the level of infraction. Disciplinary actions may include a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination of employment, depending on the severity of the violation. In addition, activities that lead to or cause the disclosure of classified information may result in criminal prosecution under the U.S. Code, Title 18, Section 798 and other applicable statutes.

FNCS managers are responsible for enforcing these practices within their areas and will be held accountable for ensuring that users are aware of and acknowledge their responsibilities.

Rules of Behavior *(ROB)* for FNCS Internal Users

FNCS User's access to information system resources indicates a level of trust between the User and FNCS Management. Therefore, Internal Users are held accountable for the following:

Rule of Behavior #1: Protect sensitive systems and data

- Users must utilize all security measures that are in place to protect the confidentiality, integrity, and availability of information and systems.
- Users must not retrieve information for, or in any other way disclose information to, someone who does not have authority to access that information.
- Users must not attempt to circumvent any security control mechanisms.
- Users who telework or remotely access FNCS information should do so only through approved remote access solutions and should safeguard all sensitive information accessed in this manner.
- Users must protect FNCS information resources when working remotely by ensuring the latest patches and antivirus software are loaded on your Government Furnished Equipment (GFE).

Rule of Behavior #2: Keep IDs and credentials secure

- Users must be responsible for all activities associated with the user's assigned user IDs, passwords, access tokens, identification badges, Personal Identity Verification (PIV) cards, or other official identification devices or methods used to gain access to FNCS data, equipment, IT systems, or facilities.

Rule of Behavior #3: Do not use prohibited software or services

- Users must access only those information systems, networks, data, control information, and software they are authorized to use.
- Users must not open email attachments or click links from unknown or suspicious sources.
- Users must avoid the introduction of harmful files/data that may contain spy-ware, viruses, etc. into any computing resource. Users must discontinue use of any system resources that show signs of being infected by a virus or other malware and report the suspected incident.

Rule of Behavior #4: Do not abuse USDA or FNCS resources

- Users must ensure the ethical use of FNCS information resources in accordance with FNCS guidelines and procedures. This includes adhering to terms of all licenses, copyright laws, contracts, and the handling of restricted information.
- Users must refrain from using FNCS information resources for inappropriate activities. Personal use of the Internet is allowed, as long as it does not interfere with official business or have an adverse effect on FNCS Information Systems.
- Users must safeguard resources against waste, loss, abuse, unauthorized users, and misappropriation.

Rule of Behavior #5: Understand and comply with USDA and FNCS information security policies and standards

- Users must attend Information Security Awareness training, as required by the USDA policy.
- Users must know who their Information System Security Managers *(ISSMs)* are and how to contact them.
- Users must report all security incidents or suspected incidents by emailing the Security Incidents Mailbox at SM.FN.Security_Incidents@usda.gov.

By your signature, you are stating that you have read, accepted, and agreed to the FNCS ROB for Internal Users. If you have any questions regarding these rules or your responsibilities outlined herein, please contact your supervisor, designated FNCS account manager, or FNCS ISO at SM.FN.SecurityOfficersMbx@usda.gov.

Rules of Behavior *(ROB)* for FNCS External Users

FNCS External User's access to information system resources indicates a level of trust between the User and USDA FNCS. Therefore, External Users of FNCS systems are held accountable for the following:

Rule of Behavior #1: Protect sensitive systems and data

- Users must conduct only authorized business within the FNCS system.
- Users' level of access to FNCS systems and networks is limited to ensure the access is no more than necessary to perform legitimate tasks or assigned duties. If you believe you are being granted access that you should not have, you must immediately contact your FNCS Point of Contact (POC) or the individual/group that provided you this form for completion.
- Users must not attempt to circumvent any security control mechanisms.

Rule of Behavior #2: Keep IDs and credentials secure

- Users must maintain the confidentiality of their authentication credentials (i.e., password). Do not reveal your authentication credentials to anyone; a FNCS employee will never ask you to reveal them.
- The system user identification (User ID/password) issued is to be used solely in connection with the performance of the user's responsibilities in support of FNCS and may not be used for personal or private gain. As a condition of receiving access, you agree to be responsible for the confidentiality of the assigned information, accountable for all activity with your user identification, and that you will notify your FNCS POC in writing upon leaving your place of employment or transfer to another position/office.
- Users must follow proper logon/logoff procedures. Manually logon to a session; do not store your credentials locally on your system or utilize any automated logon capabilities. Promptly logoff when session access is no longer needed. If a logoff function is unavailable, close the browser or application window. Never leave a computer unattended while logged into the system.

Rule of Behavior #3: Do not use prohibited software or services

- Users must not establish any unauthorized interfaces between systems, networks, and applications owned by FNCS/USDA.

Rule of Behavior #4: Do not abuse USDA or FNCS resources

- Users must ensure the ethical use of FNCS information resources in accordance with FNCS guidelines and procedures.
- Users must not browse, search, or reveal information hosted on FNCS information systems except in accordance with that which is required to perform legitimate tasks or assigned duties. Additionally, the user must not retrieve information for, or in any other way disclose information to, someone who does not have authority to access that information.
- Users must safeguard FNCS/USDA equipment, software, data, and resources in their possession from loss, theft, damage, and unauthorized use or disclosure.
- Users must adhere to all licenses, copyright laws, contracts, and other restricted or proprietary information.

Rule of Behavior #5: Understand and comply with USDA and FNCS information security policies and standards

- Users' access to FNCS Information Systems and networks is governed by, and subject to, all federal laws, including, but not limited to, the Privacy Act, 5 U.S.C. 552a. Access to FNCS systems constitutes your consent to the retrieval and disclosure of the information within the scope of your authorized access, subject to the Privacy Act and applicable state and federal laws.
- Users must understand that any person who obtains information from a computer connected to the Internet in violation of the employer's computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

By your signature, you are stating that you have read, accepted, and agreed to the FNSC ROB for External Users. If you have any questions regarding these rules or your responsibilities outlined herein, please contact your FNCS point of contact.

Form Instructions

1. **LAST, FIRST, MIDDLE NAME** - Enter the last name, first name and middle name *(if applicable)* of the person requesting FNCS computer system access. If middle name does not exist, enter n/a.

2. **TITLE** - Enter current Title.

3. **DATE OF REQUEST** - Select from the calendar, the date you are requesting access to an FNCS system.

4. **WORK EMAIL** - Enter the FNCS email address, if known.

5. **USDA E-AUTH USER ID** - Enter your official e-Authentication ID, (existing users).

   To obtain an E-Auth User ID go to the site map at https://www.eauth.usda.gov/MainPAges/eauthsitemap.aspx and click on "Create an Account"

6. **TYPE OF USER** - Select your user type from the drop-down menu; Federal, State, Contractor, or Other. “If “Other” was selected in this field, please provide an explanation in Field 20 of what “Other” means as well as the justification for the selection.”

7. **TELEPHONE**- Enter telephone.

8. **CONTRACT EXPIRATION DATE** - If you are a Contractor, enter your Contractor Expiration Date. Please contact your COTR for this date.

9. **TEMPORARY EMPLOYEE EXPIRATION DATE -** If you are a Temporary Employee *(Intern)*, enter your Expiration Date. Please contact your supervisor for this date.

10. **COMPANY/AGENCY** - Enter your company/agency affiliation.

11. **FUNCTIONAL AREA** - Enter your functional area affiliation.

12. **DIVISION/BRANCH** - Enter your division/branch affiliation.

13. **PHYSICAL DUTY LOCATION** - Select your physical duty location affiliation from the drop-down menu. Enter the physical duty street address, suite or unit number, city, state and zip code of the facility where the requesting user will be working. “If “Other” was selected in this field, please provide an explanation in Field 20 of what “Other” means as well as the justification for the selection.”

14. **SYSTEM NAME** - Please provide system description you are requesting to access.

15. **TYPE OF ACCESS / ROLE** - For the system, enter the type of access or role requested. Access and role types are system specific. Please contact AMS or System Helpdesks.

16. **ACTION REQUESTED** - Enter the type of access requested for this system, if you are not sure, please contact the system owner for the appropriate action.

17. **SYSTEM LOGIN USER ID** - If an existing account, enter in your current login ID.

18. **PROGRAM AND FORM** - This field is needed for FPRS access only. Enter the form that the user has requested to access.

19. **STATE/LOCALITY CODES** - Enter the state/locality codes that are needed for system access. State/Locality codes are FNCS organization codes that specific systems may require. If required, these codes will determine the information that you can access within the FNCS system. If you do not know your state/locality code, please contact the System Owner for the code.

20. **COMMENTS, SPECIAL INSTRUCTIONS** - Enter any comments or special instructions that are needed for the completion of this request for system access.

21. **USER ACKNOWLEDGEMENT** - Read the Privacy Act Statement and the FNCS Rules of Behavior *(ROB)*, sign and date the user acknowledgement statement. This must be completed prior to submitting this form to your supervisor.

22. **APPROVALS** - Prior to the user submitting the User Access Request form, it must be approved by the following: the user's Supervisor, the Account Manager for the system, the State Computer Security Officer, if applicable.