NATIONAL EASEMENT STAGING TOOL (NEST)
USER ACCESS PERMISSIONS REQUEST

USER INFORMATION

1. USER'S NAME *(Last, First, Middle Initial)*	**2.** USER'S TITLE	**3.** USER'S EMAIL ADDRESS
4. USER'S PHONE NUMBER	**5.** DUTY STATION *(City, State)*	**6.** SUPERVISOR'S NAME
7. SUPERVISOR'S TITLE	**8.** SUPERVISOR'S PHONE NUMBER	**9.** SUPERVISOR'S EMAIL ADDRESS

ACTION REQUESTED

10. (Check One):	**11.** USER'S eAUTHENTICATION ACCOUNT IDENTIFICATION
☐ Add New User	**(Forgot e-auth ID?)**
☐ Remove Existing User	
☐ Transfer Existing User from State:_____ to State:_____	
☐ Temporary Detail to:_____ Start:_____ End:_____	
☐ Modify User Profile, Permissions, or Roles	

USER ROLES & PERMISSIONS

12. USER'S ROLE/POSITION

☐ Administrator	☐ National Appraiser	☐ National Water Bank Program User
☐ Auditor	☐ National Data Viewer	☐ Reservation
☐ Commitment	☐ National Easement Support	☐ State Data Viewer
☐ Field Office User	☐ National Financial User	☐ State Documentation Manager
☐ Internal Control User	☐ National Program User	☐ State Program User
☐ Lead State Program User	☐ National Project Reviewer	☐ User Access Administrator
☐ Migratory Bird Habitat Initiative Auditor	☐ National Quality Assurance	

USER ACKNOWLEDGMENT

I have read the NEST Access Control Procedures and understand the security requirements of the automated information systems and applications described in this request. I understand that any violation of these procedures may result in disciplinary action, removal from the agency and USDA, and/or criminal prosecution.

13. USER'S SIGNATURE	**14.** DATE

AUTHORIZATION VERIFICATION

User's Supervisor: *I certify this user has received the NEST Access Control Procedures and I approve his or her access to NEST with the roles specified above.*

15. USER'S SUPERVISOR'S SIGNATURE	**16.** DATE

Approving Official Acknowledgement: *I certify this is the appropriate action (#10) and role (#13) for this user.*

17. STATE CONSERVATIONIST'S OR DESIGNATED APPROVING OFFICIAL'S SIGNATURE	**18.** DATE
19. NATIONAL NEST ADMINISTRATOR'S SIGNATURE	**20.** DATE

21. NOTES

Roles for NEST

National Level Roles (NHQ):

[Editable] Administrator – This role is responsible for system administration and data quality assurance processes for all data entered in NEST. This role will have permissions for general easement programs, Other Stewardship Lands, and Water Bank Program.

[Read-Only] Auditor – This role allows a user to read and search certain NEST data when needed for auditing purposes. This role will only have read and search permissions, and may have access to general easement programs, Other Stewardship Lands, and Water Bank Program depending on needs.

[Editable] Commitment – This role allows a user to administer the "Commitment Approval" page for the easement programs.

[Editable] Internal Control User – This role allows a user to implement internal control processes and quality assurance checks. This role will have access to general easement programs and Other Stewardship Lands.

[Read-Only] Migratory Bird Habitat Initiative Auditor – This role allows a user to read and search certain NEST data when needed for auditing MBHI purposes. This role will only have read and search permissions to general easement programs, and none to Other Stewardship Lands or Water Bank Program.

[Editable] National Appraiser – This role allows a user to view and edit valuation records and will able to create a valuation record and have the same permissions to reports as National Program User The role will not have permissions to Water Bank Program or Other Stewardship Lands.

[Read-Only] National Data Viewer – This role can be assigned to a user who has no role in the administration of the programs but will need to analyze general easement program data. The role will have access to all tracking inbox programs.

[Editable] National Easement Support – This role allows a user to assist with easement quality control, valuation, and procurement and will have the same permissions to reports as National Program User. This role will not have access to Water Bank Program.

[Editable] National Financial User – This role allows a user to view financial interactions with general easement programs and Water Bank Program at a National Level. This role will have no access to Other Stewardship Lands records.

[Editable] National Program User – This role allows a user to administer general easement programs and Other Stewardship Lands at a National Level. This role will not have access to Water Bank Program.

[Editable] National Project Reviewer- This role allows a user to view and edit proposed projects. Role will not have permissions to general easement programs, Water Bank Program, and Other Stewardship Lands.

[Editable] National Quality Assurance (QA) – This role allows a user to assist the NEST administrators with general easement programs. This role will have permissions for general easement programs, Other Stewardship Lands, and Water Bank Program.

[Editable] National Water Bank Program User – This role allows a user to give guidance and administer the Water Bank Program to all applicable states. This role will be allowed to permissions to Water Bank Program information only.

[Editable] Reservation – This role allows a user to administer the "Funds Certification/Reservation" page for the easement programs.

[Editable] User Access Administrator – This role allows a user to create and update NEST users within the system. This role is being created to enforce the separation of duties between a general NEST administrator and a staff member responsible for keeping user access records.

State Level Roles:

[Editable] Lead State Program User – This role allows a user to receive all emails associated with NEST information and will have the same permissions to reports as State program user. This role will have permissions for general easement programs, Other Stewardship Lands, and Water Bank Program.

[Editable] Field Office User – This role will be assigned to the field level staff. This role can edit certain data elements on the application side and in the monitoring process. This role will also be able to upload documents and enter Maintenance Request. The role will have permissions for general easement programs, Other Stewardship Lands, and Water Bank Program.

[Read-Only] State Data Viewer – This role can be assigned to a user who has no role in the administration of the programs but will need to analyze general easement program data. The role will have access to all tracking inbox programs.

[Editable] State Documentation Manager – This role allows a user to update documents for accurate documentation of activities during the easements enrollment process. This role will have permissions for general easement programs, Other Stewardship Lands, and Water Bank Program.

[Editable] State Program User – This role allows a user to have duties at all stages of the easement process. This role will have permissions for general easement programs, Other Stewardship Lands, and Water Bank Program.

NEST User Access Control Procedures

1. **USERS OF THE NRCS NATIONAL EASEMENT STAGING TOOL (NEST)** must have a User Access Permissions Request approved by their supervisor and the State conservationist, regional conservationist, deputy chief or his or her designee (if applicable) before receiving NEST user access. Requests should be submitted to the NRCS national NEST administrator for final approval and processing (NESTsupport@wdc.usda.gov).

2. **STATE CONSERVATIONISTS / APPROVING OFFICIALS WILL MAINTAIN COPIES** of the NEST User Access Permission Requests of their employees.

3. **THE STATE CONSERVATIONIST / APPROVING OFFICIAL WILL APPROVE AND SUBMIT NEST USER ACCESS REQUESTS** (within 30 days) when an authorized user's roles or duties change, when a separation from the agency occurs, to report name changes, or request profile changes. If applicable, all parties involved will be notified of any changes. Submissions should be sent to the NEST Support Outlook Box at NESTsupport@wdc.usda.gov.

4. **AUTHORIZED USERS** not using NEST for a year or that have not been certified within the last 12 months will be placed in Inactive Status.

5. **ACCESS DISTRIBUTION AND RENEWAL** must be completed securely.

6. **DO NOT ACCESS,** research, or change any account, file, record or application not required to perform the user's official duties. Users are forbidden to access their own record information, or that of a spouse, relative, friend, neighbor, or any agreement record in which she/he has a personal or financial interest. If a user is assigned to work on one of these records, she or he must contact their supervisor and behave in an ethical, technically proficient, informed, and trustworthy manner.

7. **IDENTIFY ALL** sensitive applications or data that the employee will be using in conjunction with the system and any equipment processing sensitive information to employee's supervisor, so that appropriate security measures can be implemented.

8. **RETRIEVE ALL** hard copy printouts in a timely manner. If users 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.

9. **DO NOT DISCLOSE** or discuss any USDA personnel or vendor related information with unauthorized individuals.

10. **PROMPTLY REPORT** all security incidents to user's supervisor and in accordance with 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.

Best Password Practices

DO NOT SHARE user password with others or reveal it to anyone, regardless of his or her position in or outside the USDA. Users will be held responsible if the access is not authorized. If the user thinks someone else knows their password, immediately notify the user's supervisor and the NRCS national NEST administrator. As a general rule, users should not use a computer or terminal on behalf of another person.

PROTECT USER NEST PASSWORD from disclosure. Users are responsible for any computer activity associated with their password.

DO NOT PROGRAM user login or password into automatic script routines or programs.

LOG OFF/SIGN OFF if a user goes to lunch, on break, and anytime the user leaves their computer or terminal.

References:
1. National Institute of Standards and Technology (NIST) 800-53 Revision 4
2. The Computer Security Act of 1987
3. Federal Information Security Management Act (FISMA) of 2014
4. The Privacy Act of 1974, as amended
5. Departmental Regulation 3140-001, USDA Information Systems Security Policy (May 1996)