Grantee User Account Request Form

Please use this form to request the following GrantSolutions Grantee user account actions:

- Create a new account at an existing grantee organization
- Update information pertaining to an existing grantee account
- Close an existing grantee account

GrantSolutions Grantee User Accounts
All account requests must be made by the prospective user's supervisor or other authorized organization official

1. The authorized official must complete and sign the first section of the Account Request Form.
2. The person who will be receiving access needs to:
    a. Sign and date the second part of the forms (Data Access/Security Compliance Statement)
    b. Sign and date the main signature page in the HHS Rules of Behavior.

Additional GrantSolutions Grantee User Accounts
If you require additional grantee user accounts for your organization, please complete a copy of the attached change request form for each person. Please be sure to complete the form in its entirety for each account request.

Changes to Existing GrantSolutions Grantee User Accounts
Should any information regarding an existing Grantee user account change, please complete, in its entirety, the attached change request form. Changes to existing accounts may include:

- Change of staff person's role (indicate new Job Title)
- Update of person's contact information
- Closure of an account

Requests for a change of the grant's Project Director/Project Investigator may not be completed using this form. These actions must be completed using GrantSolutions or by contacting your assigned Grants Management Specialist.

Submission of the GrantSolutions Grantee User Account Request Form
Most account changes (role assignments, new accounts, account closures) must be requested by the Grantee Authorized Official or in some cases the Program Director. The Support Center will verify all account requests as needed. Request forms sent via e-mail must be scanned to include original signatures.

Completed Grantee User Account Request Forms may be submitted to the **GrantSolutions Support Center** by email to help@grantsolutions.gov or by FAX to 301-998-7272

Initial account information will be sent to the new (or changed) user's email address provided. Upon initial login, the user will be required to change temporary password assigned by the system.

If you have any questions please contact the GrantSolutions Support Center at help@grantsolutions.gov or toll free on (866) 577-0771.

Grantee User Account Request Form

Request Type: ◯ New Account ◯ Account Change ◯ Account Closure

Partner Agency:
- ◯ Department of Health and Human Services
- ◯ Department of Agriculture
- ◯ Department of Transportation
- ◯ Other _____
- ◯ Department of State
- ◯ Social Security
- ◯ Denali Commission

Role Authority:
- ☐ Authorizing Official
- ☐ Program Director/Principal Investigator
- ☐ Support Staff
- ☐ Financial Officer
- ☐ Financial Officer Support

Organization Name: _____

Address 1: _____

Address 2: _____

City: _____ **State:** _____ **ZIP + 4:** _____

Grant Number(s): _____

This should be a grant number of any grant awarded to your organization that is or has been in GrantSolutions. This will be used to help confirm organization information.

First Name: _____ **Last Name:** _____

Title: _____

Phone: _____ **Fax:** _____

Email Address: _____

Person Address 1: _____

Person Address 2: _____

City: _____ **State:** _____ **ZIP + 4:** _____

Please complete the Person Address only if it is different from the Organization Address.

Authorized Official Name: _____

Title: _____

Authorized Official Signature: _____

Note: Request should be signed by authorized organization business/signing official.

US Government Data Access Request/Security Compliance Statement

As a user granted with Grantee authority, I agree to abide by the following:

- I will not disclose data from any GrantSolutions system to anybody except authorized system users whose roles permit access to that data.
- I will not make any unencrypted electronic copies of data from any GrantSolutions system.
- I will take all reasonable steps to ensure they do not violate the privacy and confidentiality of all data from GrantSolutions systems, and they will ensure the proper disposal of data (in any format) and printed reports.
- I will access GrantSolutions systems only to the extent that their duties require such access.
- I will abide by all HHS Rules of Behavior (See Attached).
- I will adhere to all applicable HHS and Federal Information Technology policies, including all IT security training requirements.
- I will report inappropriate or malicious use of GrantSolutions systems to the GrantSolutions Support Center and the ACF CISO/ISSO.
- I will immediately notify the GrantSolutions HelpDesk of any account changes, including the need to close my account.

User Name (Printed) _____

User Signature _____ Date _____

HHS Rules of Behavior

The Department of Health and Human Services (HHS) *Rules of Behavior* (HHS RoB) provides appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users. The HHS RoB, in conjunction with the HHS-OCIO (2006-0001) *Policy for Personal Use of Information Technology Resources*, dated February 17, 2006, and are issued under the authority of the HHS-OCIO (2009-0003) *Policy for Information Systems Security and Privacy*, dated June 25, 2009. Both policy references are located at http://www.hhs.gov/ocio/policy/index.html. The HHS-OCIO-2008-0003.001S, HHS *Rules of Behavior*, dated February 12, 2008, is obsoleted by this issuance which adds a signature page for Privileged User accounts.

All users of HHS information technology resources must read these rules and sign the accompanying acknowledgement form before accessing Department data/information, systems and/or networks. This acknowledgement must be signed annually, preferably as part of the HHS Information Systems Security Awareness Training, to reaffirm knowledge of, and agreement to adhere to the HHS RoB. The HHS RoB may be presented to the user in writing or electronically, and the user's acknowledgement may be obtained by written or electronic signature. Each Operating Division (OPDIV) Chief Information Officer (CIO) shall determine how signatures are to be submitted, retained, and recorded[1]; and may append any necessary information or fields to the signature page. For electronic signatures, the specific version number of the HHS RoB must be retained, along with the date and sufficient identifying information to uniquely link the signer to his or her corresponding information system accounts. Electronic copies of the signed signature page may be retained in lieu of the original. Each OPDIV CIO shall ensure that information system and information access is prohibited in the absence of a valid, signed acknowledgement of the HHS RoB from each user.

These rules cannot account for every possible situation. Therefore, personnel shall use their best judgment and highest ethical standards to guide their actions.

Non-compliance with the HHS RoB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include one or more of the following actions:

- Suspension of access privileges; revocation of access to federal information, information systems, and/or facilities;
- Reprimand;
- Termination of employment;
- Removal or debarment from work on Federal contracts or projects;
- Monetary fines; and/or
- Criminal charges that may result in imprisonment.

HHS OPDIVs may require users to acknowledge and comply with OPDIV-level policies and requirements, which may be more restrictive than the rules prescribed herein.

Furthermore, supplemental rules of behavior may be created for specific systems which require users to comply with rules beyond those contained in this document. In such cases, users must also sign these supplemental rules of behavior prior to receiving access to these systems, and must comply with any ongoing requirements of each individual system to retain access (such as re-acknowledging the system-specific rules by signature each year). System owners shall document system-specific rules of behavior and any recurring requirement to sign the respective acknowledgement in the Security Plan for their systems. Each OPDIV CIO shall implement a process to obtain and retain the signed rules for such systems and shall ensure that user access to such system information is prohibited without a signed acknowledgement of system-specific rules and a signed acknowledgement of the HHS RoB.

National security systems, as defined by the Federal Information Security Management Act (FISMA), must independently or collectively implement their own system-specific rules.

These HHS RoB apply to local, network, and remote use[2] of HHS information (in both electronic and physical forms) and information systems by any individual.

I assert my understanding that:

- Information and system use must comply with Department and OPDIV policies and standards, and with applicable laws;
- Use for other than official, assigned duties is subject to the HHS-OCIO-2006-0001, *Policy for Personal Use of IT Resources*, dated February 17, 2006;
- Unauthorized access to information or information systems is prohibited; and
- Users must prevent unauthorized disclosure or modification of sensitive information.[3]

I shall:

- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on HHS systems;
- Abstain from loading unapproved software from unauthorized sources[4] on Department systems or networks;
- Wear identification badges at all times in Federal facilities;
- Log-off or lock systems when leaving them unattended;
- Use provisions for access restrictions and unique identification to information and avoid sharing accounts;
- Complete security awareness training before accessing any HHS system and on an annual basis thereafter, and complete any specialized role-based security or privacy training, as required by HHS policies;
- Permit only authorized HHS users to use HHS equipment and/or software;
- Secure sensitive information (media neutral) when left unattended;
- Keep sensitive information out of sight when visitors are present;
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with the HHS-OCIO-2007-0004, *Policy for Records Management*, dated January 30, 2008 and sanitization policies, or as otherwise directed by management;

- Only access sensitive information necessary to perform job functions (i.e., need to know);
- Use Personally Identifiable Information (PII) only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published System of Records Notices;
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary, to assure fairness in making determinations about an individual;
- Adequately protect any sensitive information entrusted to me;
- Protect HHS information assets[5] (HHS assets include but are not limited to hardware, software, and federal records) from unauthorized access, use, modification, destruction, theft, or disclosure and shall treat such assets in accordance with any information handling policies;
- Properly protect (i.e., encrypt) HHS sensitive information, to include sensitive information sent via email; and
- Immediately report to the OPDIV Chief Information Security Officer (CISO) all: lost or stolen HHS equipment from the agency premises without proper authorization; known or suspected security incidents; known or suspected information security policy violations or compromises; or suspicious activity in accordance with OPDIV procedures. Known or suspected security incidents involve the actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information maintained or in possession of HHS or information processed by contractors and third parties on behalf of HHS.

I shall not:

- Violate, direct, or encourage others to violate HHS policies or procedures;
- Circumvent security safeguards including violating security policies or procedures or reconfigure systems except as authorized (i.e., violation of least privilege);
- Use another person's account, identity, or password;
- Remove computers or equipment from the agency premises without proper authorization;
- Send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums;
- Exceed authorized access to sensitive information;
- Store sensitive information in public folders or other insecure physical or electronic storage locations;
- Share or disclose sensitive information except as authorized and with formal agreements that ensure third parties will adequately protect it;
- Transport, transmit, email, remotely access, or download sensitive information unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information;
- Use sensitive information for anything other than the purpose for which it has been authorized;
- Access information for unauthorized purposes;
- Use sensitive HHS data for private gain or to misrepresent myself or HHS or any other unauthorized purpose;

- Store sensitive information on mobile devices[6] such as laptops, personal digital assistants (PDAs), universal serial bus (USB) drives, or on remote/home systems without authorization and/or appropriate safeguards (i.e., HHS approved encryption);
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for myself or others;
- Copy or distribute intellectual property—including music, software, documentation, and other copyrighted materials—without permission or license from the copyright owner;
- Modify or install software without prior management approval;
- Load unapproved software from unauthorized sources[7] on Department systems or networks;
- Use a personal email system (i.e., Gmail, Yahoo, Hotmail) to transmit sensitive information; and
- Use systems without the following protections engaged to access sensitive HHS information:
    - Antivirus software with the latest updates;
    - Anti-spyware and personal firewalls installed on personally-owned systems;
    - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access and mobile devices ; and
    - Approved encryption to protect sensitive information stored on mobile devices or recordable media, including laptops, USB drives, and external disks; stored on remote or home systems; or transmitted or downloaded via e-mail or remote connections.

The following are prohibited on Federal Government systems per the HHS-OCIO-2006-0001*Policy for Personal Use of Information Technology Resources*, dated February 17, 2006:

- Unethical or illegal conduct;
- Sending or posting obscene or offensive material in messages or forums;
- Sending or forwarding chain letters, email spam, inappropriate messages, or unapproved newsletters and broadcast messages;
- Sending messages supporting political activity restricted under the Hatch Act;
- Conducting any commercial or “for-profit” activity;
- Utilizing peer-to-peer software except for secure tools approved in writing by the OPDIV CIO to meet business or operational needs;
- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive text or images, or other offensive material;
- Creating and/or operating unapproved Web sites;
- Incurring more than minimal additional expense, such as using non-trivial amounts of storage space or bandwidth for personal files or photos; and
- Using the Internet or HHS workstation to play games, visit chat rooms, or gamble.

I shall ensure passwords:

- Are complex, and contain a minimum of eight alphanumeric characters and at least one uppercase and one lowercase letter, one number, and one special character;
- Do not contain or consist of common words, names, or user IDs;
- Are changed immediately in the event of known or suspected compromise, and immediately upon system installation (e.g., default or vendor-supplied passwords);
- Are not reused until at least six other passwords have been used; and
- Are committed to memory, or stored in a secure place.

SIGNATURE PAGE

I have read the *HHS Rules of Behavior* (HHS RoB), version 2010-0002.001S, dated August 26 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Name:_____

User's Signature:_____

Date Signed:_____

---

[1] A privacy impact assessment (PIA) is required for collecting this information. The PIA should be used in determining if a System of Records Notice (SORN) is required. See *HHS Policy for Privacy Impact Assessment (PIA)*, located at: http://www.hhs.gov/ocio/policy/index.html.

[2] Refer to the Glossary of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, dated August 2009, for definitions of local, network, and remote access.

[3] HHS definition of sensitive information is defined in the HHS Memorandum: *Updated Departmental Standard for the Definition of Sensitive Information* (as amended) available upon request.

[4] An unauthorized source is any location (e.g., file store or server to which a device could connect, Internet site, Intranet site) or process that is not permitted by HHS or OPDIV/STAFFDIV IT security personnel for the distribution of software.

[5] HHS IT assets are defined as hardware, software, systems, services, and related technology assets used to execute work on behalf of HHS. Definition is adapted from NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, dated July 2002.

[6] Refer to the Glossary of NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, dated August 2009, for the definition of mobile device.
[7] Ibid.