ADMINISTRATION FOR CHILDREN & FAMILIES
Office of the Chief Information Officer

Runaway and Homeless Youth – Homeless Management Information System (RHY-HMIS) User Access Request Form

Instructions: In order to provide you (the requestor) access to RHY-HMIS, please complete Part A, read the RHY-HMIS Rules of Behavior in part B, provide your signature in Part C, and your approvers signature in Part D of this form.

Part A: Please fill in request type and requestor information and sign on page 5

Account Type: ☐ New Account ☐ Modification of Account ☐ Removal of Account	**Account Role:** ☐ Grantee User ☐ Grantee Manager ☐ Federal Project Officer (FPO) ☐ FYSB Lead ☐ RHY-HMIS Administrator (*Abt Associates Administrators only*)
First Name:	Last Name:
Email:	
Contact Number:	
Organization:	
Security Awareness Training Completion Date: Select Date	
Justification for Access:	

Part B: Rules of Behavior (RoB) for Runaway and Homeless Youth – Homeless Management Information System (RHY-HMIS)

This Runaway and Homeless Youth- Homeless Management Information System (RHY-HMIS) serves the Administration for Children and Families (ACF) of the Department of Health and Human Services (HHS), stakeholders, and users. The purpose of RHY-HMIS is to capture information on critical issues, services, demographics, and other characteristics of the runaway and homeless youth. As a RHY-HMIS user, you agree to the following:

These Rules of Behavior (RoB) for General Users apply to all RHY-HMIS and Department of Health and Human Services (HHS) employees, contractors, and other personnel who have access to HHS information resources and information technology (IT) systems.

Users of HHS information and information systems shall read, acknowledge, and adhere to the following rules prior to accessing data and using HHS information and systems.

A. HHS Information Systems:

When using and accessing HHS information resources and systems, I understand that I must:

1. Comply with federal laws, regulations, and HHS/Operating Division (OpDiv) policies, standards, and procedures and that I must not violate, direct or encourage others to violate HHS policies, standards or procedures;
2. Not allow unauthorized use and access to HHS information and information systems;
3. Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing;
4. Limit personal use of information and IT Resources to the extent that it does not:
    a. disrupt my productivity,
    b. interfere with the mission or operations of HHS, and
    c. violate HHS security and privacy policies;
5. Have no expectation of privacy while using and accessing HHS information resources and assets at any time, and I understand that any actions and activities are subject to HHS monitoring, recording, and auditing;
6. Complete all mandatory training (e.g., security and privacy awareness, role-based training, etc.) prior to accessing HHS systems and periodically thereafter as required by HHS policies;
7. Be accountable for my actions while accessing and using HHS information, information systems and IT resources;
8. Not share passwords or provide passwords to anyone, including system administrators. I must protect my passwords, Personal Identity Verification (PIV) card, Personal Identification Numbers (PIN) and other access credentials from disclosure and compromise;
9. Promptly change my password when required by HHS policy and if I suspect that it has been compromised;
10. Not use another person's account, identity, password/passcode/PIN, or PIV card or allow others to use my GFE and/or other HHS information resources provided to me to perform my official work duties and tasks
11. Reconfigure systems and modify GFE, install/load unauthorized/unlicensed software or make configuration changes without proper official authorization;
12. Properly secure all GFE, including laptops, mobile devices, and other equipment that store, process, and handle HHS information, when leaving them unattended either at the office and other work locations, such as home, hoteling space, etc. and while on travel. This includes locking workstations, laptops, placing GFE in locked drawer, cabinet, or simply out of plain sight, and removing my PIV card from my workstation.
13. Only use authorized credentials, including PIV card, to access HHS systems and facilities and will not attempt to bypass access control measures; and
14. Report all suspected and identified information security incidents and privacy breaches to the Helpdesk, Incident Response Team (IRT) and/or Privacy Incident Response Team (PIRT) as soon as possible, without unreasonable delay and no later than within ***one (1) hour*** of occurrence/discovery

B. Data Protection:

When handling and accessing HHS information, I understand that I must:

1. Take all necessary precautions to protect HHS information and IT assets, including but not limited to hardware, software, sensitive information, including but not limited to Personally Identifiable Information (PII), Protected Health Information (PHI), federal records [media neutral], and other HHS information from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and in accordance with HHS Policies
2. Protect sensitive information (e.g., sensitive information, such as confidential business information, PII, PHI, financial records, proprietary data, etc.) at rest (stored on laptops or other computing devices) regardless of media or format, from disclosure to unauthorized persons or groups. This includes, but is not limited to:
    a. Never store sensitive information in public folders, unauthorized devices/services or other unsecure physical or electronic locations,
    b. Always encrypt sensitive information and in transit (transmitted via email, attachment, media, etc.),
    c. Always disseminate passwords and encryption keys out of band (e.g., via text message, in person, or phone call) or store password and encryption keys separately from encrypted files, devices and data when sending encrypted emails or transporting encrypted media
    d. Access or use sensitive information only when necessary to perform job functions, and do not access or use sensitive information for anything other than authorized purposes, and
    e. Securely dispose of electronic media and papers that contain sensitive data when no longer needed, in accordance with the HHS Policy for Records Management and federal guidelines;
3. Immediately report all suspected and known security incidents (e.g., GFE loss or compromise, violation of security policies, etc.), privacy breeches (e.g., loss, compromise or unauthorized access and use of PII/PHI), and suspicious activities to the Helpdesk and/or CSIRC/CSIRT pursuant to HHS incident response policy and/or procedures.

C. Privacy:

I understand that I must:

1. Collect information about individuals only as required by my assigned duties and authorized by a program-specific law, after complying with any applicable notice or other requirements of laws such as the Privacy Act of 1974, the Paperwork Reduction Act, and agency privacy policies and OMB memoranda, such as OMB Memorandum M-17-06 governing collection of PII on agency websites;
2. Release information to members of the public (including individuals, organizations, the media, individual Members of Congress, etc.) only as allowed by the scope of my duties, applicable HHS policies, and the law
3. Not access information about individuals unless specifically authorized and required as part of my assigned duties
4. Not use non-public HHS data for private gain or to misrepresent myself or HHS or for any other unauthorized purpose;
5. Use information about individuals (including PII6 and PHI7) only for the purposes for which it was collected and consistent with conditions set forth in stated privacy notices such as those provided to individuals at the point of data collection or published in the Federal Register (to include System of Records Notices [SORNs]);
6. Ensure the accuracy, relevance, timeliness, and completeness of information about individuals, as is reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual; and
7. Maintain no record describing how an individual exercises his or her First Amendment rights, unless it is expressly authorized by statute or by the individual about whom the record is maintained, or is pertinent to and within the scope of an authorized law enforcement activity.

D. Strictly Prohibited Activities:

When using RHY-HMIS I must refrain from the following:

1. Unethical or illegal conduct (e.g. pornography, criminal and terrorism activities, and other illegal actions and activities);
2. Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages except when forwarding to report this activity to authorized recipients;
3. Sending messages supporting or opposing partisan political activity as restricted under the Hatch Act and other federal laws and regulations;
4. Using peer-to-peer (P2P) software except for secure tools approved in writing by the OpDiv CIO (or designee) to meet business or operational needs;
5. Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive or pornographic text or images, or other offensive material (e.g. vulgar material, racially offensive material, etc.);
6. Creating and/or operating unapproved/unauthorized Web sites or services;
7. Using, storing, or distributing, unauthorized copyrighted or other intellectual property;
8. Using HHS information, systems, and devices to send or post threatening, harassing, intimidating, or abusive material about anyone in public or private messages or any forums;
9. Exceeding authorized access to sensitive information:
10. Using HHS GFE for commercial or for-profit activity, shopping, instant messaging (for unauthorized and non-work related purposes), playing games, gambling, watching movies, accessing unauthorized sites, and hacking;
11. Using an official HHS e-mail address to create personal commercial accounts for the purpose of receiving notifications (e.g., sales discounts, marketing, etc.), setting up a personal business or website, and signing up for personal memberships. Professional groups or memberships related to job duties at HHS are permissible;
12. Removing data or equipment from the agency premises without proper authorization;
13. Sharing, storing, or disclosing sensitive information with third-party organizations and/or using third-party applications (e.g. DropBox, Evernote, iCloud, etc.) unless authorized and with formal agreement in accordance with HHS policies;
14. Transporting, transmitting, e-mailing, texting, remotely accessing, or downloading sensitive information unless such action is explicitly permitted in writing by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information; and
15. Knowingly or willingly concealing, removing, mutilating, obliterating, falsifying, or destroying HHS information.

E. For Privileged Users:

A Privileged User is a user who has been granted significantly elevated privileges for access to protected physical or logical resources. A privileged user has the potential to compromise the three security objectives of confidentiality, integrity, and availability. Such users include security personnel or system administrators who are responsible for managing restricted physical locations or shared IT resources and have been granted permissions to create new user accounts, modify user privileges, as well as make system changes. Examples of privileged users include:

- Application developer
- Database administrator
- Domain administrator
- Data center operations personnel

- IT tester/auditor
- Helpdesk support and computer/system maintenance personnel
- Network engineer
- System administrator

I understand that as a Privileged User of RHY-HMIS, I must:

- Use Privileged User accounts appropriately for their intended purpose and only when required for official administrative actions.
- Use multi-factor authentication when logging into the Environment.
- Use Government Furnished Equipment (GFE) when logging into the Environment.
- Protect all Privileged User account passwords/passcodes/Personal Identity Verification (PIV)/Personal Identified Numbers (PINs) and other login credentials used to access ACF information systems.
- Comply with all system/network administrator responsibilities in accordance with the HHS IS2P and any other applicable policies.
- Notify system owners immediately when privileged access is no longer required.
- Properly protect all sensitive information and securely dispose of information and GFE that are no longer needed in accordance with HHS/ACF sanitization policies.
- Report all suspected or confirmed information security incidents (security and privacy) to the ACF Incident Response Team and my supervisor as appropriate.
- Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a Privileged User of RHY-HMIS, I must not:

- Share Privileged User account(s), password(s)/passcode(s)/PIV PINs and other login credentials.
- Install, modify, or remove any system hardware or software without official written approval or unless it is part of my job duties.
- Remove or destroy system audit logs or any other security event log information unless authorized by appropriate official(s) in writing.
- Tamper with audit logs of any kind. Note: In some cases, tampering can be considered evidence and can be a criminal offense punishable by fines and possible imprisonment.
- Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls for unauthorized purposes.
- Introduce unauthorized code, Trojan horse programs, malicious code, viruses, or other malicious software into ACF information systems or networks.
- Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses.
- Use Privileged User account(s) for day-to-day communications and other non-privileged transactions and activities.
- Elevate the privileges of any user without prior approval from the system owner.
- Use privileged access to circumvent ACF policies or security controls.
- Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals.
- Use a Privileged User account for Web access except in support of administrative related activities.
- Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner.
- Use systems (either government issued or non-government) without the following protections in place to access sensitive ACF information:
    - Antivirus software with the latest updates
    - Anti-spyware and personal firewalls
    - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access
    - Approved encryption to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

Part C: Requestor Signature

By signing this form, I certify that understand that my User ID, password, and token are to be kept confidential and secure; should I share this information, my ID will be revoked. I have read the above Rules of Behavior (RoB) for users of RHY-HMIS and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or ACF information security policies and standards may result in disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to these RoB must be authorized in advance in writing by the designated authorizing official(s). I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which these RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.		
Name:	Signature: X	Date: Select Date

Part D: Verification and Approvals

By signing this form, I validate that all required criteria have been met by the requestor in order to obtain access to RHY-HMIS.

☐ User has completed annual security awareness training within the past 365 days and signed the Rules of Behavior.

Account Type	Approver's Signature	Date
Grantee User account	**Grantee Manager:** X	Date: Select Date
Grantee Manager account Federal Project Officer account (FPO) FYSB Lead account	**ACF/FYSB Federal Staff/System Owner:** X	Date: Select Date
RHY-HMIS Administrator account (*Abt Associates Administrator Only*)	**ACF/FYSB System Owner:** X	Date: Select Date