



Energy Programs Service Provider eHEAT Administrator Security Agreement



Description:

This agreement specifies the expectations and responsibilities of the Service Provider Security Administrator to carry out the administration responsibilities related to use of the eHEAT system.

The eHEAT system security allows only authorized Service Provider employees (“users”) to perform the tasks and processes necessary to deliver the Energy Assistance Program (EAP) and the Weatherization Assistance Program (WAP). Service Provider eHEAT Security Administrators authorize users by giving them specific access to the necessary system function(s) on the eHEAT system.

Background:

The Service Provider Security Administrator assigns each authorized user one or more roles that parallel employee functions for EAP and WAP delivery.

The eHEAT system has one central State Security Administrator. The State Security Administrator establishes roles for Department of Commerce (Commerce) users and Service Provider Security Administrators and Energy Vendor Security Administrators.

Roles and Responsibility:

The Service Provider Security Administrator is responsible to ensure only authorized users have access to and are utilizing the eHEAT system. The Service Provider Security Administrator’s role is to monitor and manage all eHEAT users within his/her Service Provider. The Service Provider Security Administrator is authorized to perform the following tasks:

- Creating new users
- Editing users
- Resetting password for the users
- Disabling users on leave, laid off, on vacation, terminated or reassigned to non-EAP duties
- Enabling users
- Creating new roles
- Editing roles
- Assign functions to roles
- Assigning roles to users

Terms:

- User. An individual who can log on and view or act on eHEAT data.
- Group. A named collection of eHEAT users. eHEAT has four groups: Commerce, Commerce Fiscal, Service Providers, and Vendors.
- Role. A named collection of functions in the eHEAT System.
- Function. An action or set of actions, such as “View Application” or “Enter Consumption.”

Energy Programs Service Provider eHEAT Administrator Security Agreement (page 2)

To ensure secured and authorized access to the eHEAT system, the Service Provider Security Administrator agrees to:

- Maintain the confidentiality of his/her User ID and Password.
- Create users only for individuals authorized to deliver the program.
- Manage Service Provider User Security Agreements and make them available to State Staff upon request.
- Follow all policies and practices established by EAP, WAP and the Service Provider, including data access and data sharing policies and procedures in accordance with the following:
 - Minnesota Statute Section 216C.266 provides that data collected maintained or created because an individual applies for energy assistance is private data pursuant to the Minnesota Government Data Practices Act (MGDPA) (Minnesota Statute Section 13.01). The collection, storage, use and release of the information shall be limited to that necessary for the administration and management of the program. The information may not be released except as permitted by the MGDPA.
- Disable users immediately upon termination of their role in service delivery or upon becoming aware of a user's inappropriate or unauthorized use of the eHEAT system.
- Immediately report known or suspected security breaches to State Security Administrator.
- Monitor user roles for appropriate usage.
- Immediately report changes to his or her status to the State Security Administrator.

By signing this I agree to comply with all requirements of the Service Provider Security Administrator described above, and acknowledge and agree to the following:

The eHEAT system is the property of Commerce. Access to this service is for authorized personnel only. Use of this system without authority or in excess of authority from Commerce may result in disciplinary action, civil and criminal sanctions and other appropriate action. Any activity on this system may be monitored or accessed by Commerce or other authorized officials at any time. This includes any data created or stored using this system. All such data is subject to the MGDPA. Access or use of the data without the expressed authorization of the State Security Administrator is a violation of the MGDPA. Further, the State of Minnesota prohibits unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of its information in accordance with the Minnesota Statutes Sections 609.87 - 609.891.

Service Provider Security Administrator's Printed Name: _____
Last four digits of the Service Provider Security Administrator's Soc. Security Number: _____
Service Provider Security Administrator's Agency: _____
Service Provider Security Administrator's Phone: _____
Service Provider Security Administrator's Email: _____
Service Provider Security Administrator's Signature: _____
Date Signed: _____

Effective for Federal Fiscal Year 2017