

Ginnie Mae Enterprise Portal (GMEP) User Registration for Custodian ONLY

Instructions

- (1) Complete the information in the boxes below – please print.
- (2) Select the requested roles(s).
- (3) Read the User Rules of Behavior.
- (4) Sign and date this registration request.
- (5) Have your supervisor sign this registration request.
- (6) Submit this request to your Security Officer for processing.

| | | |
|--------------------|--------------------------|-------------------|
| Organization Name: | | |
| User Last Name: | First Name: | Middle Name: |
| Name Suffix: | Prefix: (Mr., Ms., Mrs.) | Office Phone No.: |
| Office E-Mail: | | Fax No.: |

Select Roles (Select All That Apply):

| | |
|--|---|
| <input type="checkbox"/> MAMS Document Custodian User Access to retain the physical document of the Master Agreement. | <input type="checkbox"/> PTS Document Custodian Report Access Access to view reports. |
| <input type="checkbox"/> RSA Token Holder Provide means for users to test their token access. | <input type="checkbox"/> eNotification User e-Notification (eN) |
| <input type="checkbox"/> RSA Temporary Bypass Provide means for token holder to authenticate if they have forgotten or lost their token. | |

USER RULES OF BEHAVIOR

As a user of the GMEP, I understand that I am personally responsible for all use and any misuse of my user account and password. I understand that by accessing a U.S. Government information system, I must comply with the following requirements:

- (1) Users must safeguard the information to which you have access at all times.
- (2) The system may be used only in support of Ginnie Mae business.
- (3) The system may not be used for any purpose other than those functions related to Ginnie Mae's business.
- (4) The government reserves the right to monitor the activities of any user and/or any machine connected to GMEP.
- (5) The GMEP and the information contained within are the property of the federal government. Ginnie Mae owns the data stored on these systems, including all messages and information, even those deemed personal.
- (6) No data may be transmitted on the system that is more sensitive than the level for which that system has been approved.
- (7) Information that was obtained via GMEP may not be divulged outside of government channels without the express, written permission of the system owner.
- (8) Any activity that would discredit Ginnie Mae, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material, is prohibited.
- (9) Any activity that violates Federal laws for information protection (e.g., reconnaissance techniques, hacking, phishing, spamming, etc.), is expressly prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.
- (10) GMEP user accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism should never be shared or stored any place easily accessible. If a password is stored it may not be stored in a clear-text or readable format. Sharing of user accounts is grounds for terminating system access.
- (11) Per Ginnie Mae Policy, GMEP has the following password format requirements:
Passwords must be at least eight (8) alphanumeric characters in length, and contain the following five (5) character types:
 - Maximum twenty (20) characters in length;
 - Must have at least one (1) English upper case letter (A, B, C, etc.);
 - Must have at least one (1) English lower case letter (a, b, c, etc.);
 - Must have at least one (1) Arabic number (0, 1, 2, 3, etc.);
 - Must have at least one (1) special character from the following set: (! @#\$%^&*()_+).
- (12) Passwords should not be created using the following:
 - Dictionary words or common names, such as Betty, Fred, Rover;
 - Portions of associated account names, for example, user ID, login name;
 - Consecutive character strings, such as abcdef, 123456;

- Simple keyboard patterns, such as asdfgh, qwerty;
 - Generic passwords, such as a password consisting of a variation of the word “password” (e.g., P@ssword1).
- (13) Passwords must be changed every ninety (90) days and should never be repeated.
- (14) Password history will prevent users from using the same password from the previous (24) password changes.
- (15) After three (3) invalid password attempts, the user account will be locked. The user must contact the appropriate Help Desk or Security Officer in person for identification verification and to unlock the account.
- (16) The user’s Supervisor and Security Officer must authorize and approve the employee's level of access in writing via documented account management procedures.
- (17) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), pre-public release information such as economic indicators, proprietary data, or export controlled software or data is prohibited. All use of copyrighted software must comply with copyright laws and license agreements.
- (18) Remote off-site, (e.g., dial-in, VPN) access to GMEP Administrative Functions must be approved and authorized in writing by the appropriate management authority and the Ginnie Mae Information System Security Officer.
- (19) Authorized users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time.
- (20) At no time should personally owned equipment be connected to the system.
- (21) Any security problems or password compromises must be reported immediately to the appropriate Help Desk or Security Officer.
- (22) I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to ten (10) years in jail for the first offense for anyone who commits any of the following violations:
- Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.
 - Intentionally, without authorization, accesses a government information system and impacts the government’s operation, including availability of that system.
 - Intentionally accesses a government information system without authorization, and alters, damages, or destroys information therein.
 - Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.
- (23) Screen-savers must be password protected.
- (24) Movable media, (such as diskettes, CD-ROMs, and Zip disks), that contain sensitive and/or official information must be secured when not in use.
- (25) When the user no longer has a legitimate need to access the system, the user must notify his/her Supervisor. The Supervisor must notify the Security Officer immediately in writing so that access can be terminated. The Security Officer will notify the Ginnie Mae Security Administrator.

- (26) Upon initial login I will be required to select and answer three (3) Security questions for future use to change or reset my password.
- (27) If your Security Officer issues a one-time password token (e.g. RSA Token) or other secondary authentication device, you accept the responsibilities and obligations presented on the forms and documents provided when the device is issued. This includes but is not limited to initiation, usage, storage, return, and reporting procedures for the authentication device.

Actions violating any of these rules will result in immediate termination of your assigned identifier/password from the system.

USER CERTIFICATION:

I have read the above statement of policy regarding system security awareness and practices when accessing GMEP's information resources. I understand the policies as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the Ginnie Mae's computer resources.

User Signature

Date

SUPERVISOR CERTIFICATION:

I certify that I have been designated as an authorized Supervisor to approve user registration forms by my organization and will abide by all of the policies and rules as set forth by Ginnie Mae. I will make sure that I only assign active employees as users and to the best of my knowledge there will be no sharing of IDs. I will verify the identity of the user by the approved listing of identification. I understand that all accounts will be accessing government information systems.

I recognize that a violation of this certification could result in disciplinary action against my organization.

Verify User Phone number

Verify User E-Mail address

CERTIFIED BY:

Supervisor Name

Supervisor Phone Number

Supervisor Signature

Date

FOR SECURITY OFFICER USE ONLY

SECURITY OFFICER CERTIFICATION:

Authorized Supervisor Called-Back

Verified User and Permissions

1st Security Officer Name

Officer Phone Number

1st Security Officer Signature

Date

User Registration Approved

User Added to the Portal

2nd Security Officer Name

Officer Phone Number

2nd Security Officer Signature

Date