Ginnie Mae Enterprise Portal (GMEP)
User Registration Form

Instructions

(1) Complete the information below.
(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	
Last Name	
First Name	
Middle Name	
Office Phone No.	
Office Email	
Fax No.	

Select Roles (Select All That Apply):

RFS

☐ **Upload & Exception Feedback User**	☐ **Pool Accounting User**	☐ **SCRA User**	☐ **GPADS User**	☐ **HMBS User**	☐ **e-Notification User**	☐ **IOPP User**
Exception feedback	Pool Accounting - Single Family	Servicemembers Civil Relief Act (SCRA)	Issuer feedback	For pool accounting and reporting	Communication and system generated announcements	Issuer feedback
Matching and Suspense (MAS)	Pool Accounting – Multifamily	File upload				
File upload	Exception feedback					
	Matching and Suspense (MAS)					
	File upload					

IPMS

☐ **RPN Issuer**	☐ **CM Issuer**	☐ **PTS Issuer**	☐ **RSA Token Holder**
Enter pool number request	View requests and reports	*Selling Issuer*: Submit request for Transfer	Provide means for users to test their token access.
Request maximum pool number calculation override	Request commitment and accept commitment fee	*Buying Issuer*: Accept and authorize Transfer	
View reports			
☐ **MAMS Issuer**	☐ **MAMS Subservicer**	☐ **MAMS Participation Agent**	☐ **RSA Temporary Bypass**
Search and view agreements and reports	View HUD-11707 agreements where Issuer is Subservicer	View HUD-11703-II agreements where Issuer is Subservicer	Provide means for token holder to authenticate if they have forgotten or lost their token.
Create and submit agreements	Search HUD-11707 agreements where Issuer is Subservicer	Search HUD-11703-II agreements where Issuer is Subservicer	
Upload documents	Submit HUD-11707 agreements where Issuer is Subservicer	Submit HUD-11703-II agreements where Issuer is Subservicer	

USER RULES OF BEHAVIOR

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

(1) Users must:

a. Safeguard the information to which you have access at all times.

b. Obtain your supervisor's written approval prior to taking any Ginnie Mae sensitive information home or otherwise away from the office. The supervisor's approval must identify the business necessity for removing such information.

c. Adhere to the security policies and procedures when approval is granted to take sensitive information home or away from the office.

(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) The user's Supervisor and Security Officer must authorize and approve the employee's level of access in writing via documented account management procedures.

(12) 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.

(13) 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.

(14) Authorized users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time.

(15) At no time should personally owned equipment be connected to the system.

(16) Any security problems or password compromises must be reported immediately to the appropriate Help Desk or Security Officer.

(17) 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.

(18) 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.

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**