Fannie Mae

Best Practices for Administrators

This document describes recommended best practices for organizations with access to Fannie Mae technology applications. The following information describes tips for reviewing Administrator access, protecting user credentials and tips for password expirations.

Technology Application Access Review Tips for Administrators

It is a recommended best practice for organizations to review their employees' access to Fannie Mae technology applications on a regular basis to ensure that it is secure and commensurate with job responsibilities.

Why is it important to review user access?

Regulatory compliance requirements and security policies increasingly demand that organizations maintain effective controls over who has access to sensitive corporate and customer information. Complying with these requirements can be challenging, as users often have unique and changing business responsibilities, accumulating access over time that they no longer need, but do not remove.

Reviewing user access on a regular basis enables an organization to help meet its compliance and security policies by validating existing access and flagging questionable entitlements for possible change or removal.

What information should be reviewed?

Users should be reviewed at a minimum for the following information:

- First and Last Name: the name of the user registered in Fannie Mae's system of record.
- User ID: the ID with which the user logs in to all assigned Fannie Mae applications.
- Phone Number: the phone number at which the user may be reached.
- E-mail address: the e-mail address to which system communication, such as security notifications, is sent.
- Application: Fannie Mae application(s) to which the user has access.
- Role: the specific authorization role(s) assigned to the user for the associated application.
- Last log-in date: the date of the user's last successful log in to any Fannie Mae application.

What are the best practice guidelines for access reviews?

As access is reviewed, the following should be considered:

- Is the user still employed by your company?
- Has the job responsibility of the user changed?
- Should the user still have access to any Fannie Mae technology?
- Should the user still have access to a particular Fannie Mae application?
- Should the user still have the assigned roles for the application?

How can organizations review access for Fannie Mae technology?

User access information is reviewed through Technology Manager Administrator functionality. It is used to create and manage user-level access to selected Fannie Mae technology applications. More information on Technology Manager can be found on the Business Portal.

Protecting User Credentials

Fannie Mae strongly encourages you to review your staffs' user credentials on a regular, pre-determined basis. This regular review will help you ensure Fannie Mae systems and the data contained within them is secure and protected. Specifically, you should:

- Ensure each employee utilizes a user ID and password that belongs only to them; do not share user IDs and passwords;
- Delete a user ID immediately if an employee transitions to a new position, resigns, or is terminated from the company; and
- Remove or change application and/or user access if an employee's role changes.

As a reminder, the 4-digit numerical user PIN is required for all user ID password resets. Users are encouraged to keep a record of that PIN in a secure location for easy retrieval.

Finally, we recommend you review your company's Technology Manager Corporate and User Administrators on a regular basis (at least quarterly) to ensure those roles are filled appropriately and with trained Technology Manager users and your staff know who to contact for access updates and password resets. Corporate Administrators have the ability to authorize technology contracts on your company's behalf. Regularly review the list of staff in this role to ensure appropriate assignments.

Off-Shore Use

Off-shore use of Fannie Mae technology applications is not permitted. Access and use of Fannie Mae technology applications is limited to the U.S., Guam, the Virgin Islands and Puerto Rico, per the terms of the Fannie Mae Software Subscription Agreement.

Use by Contractors

Individuals who are hired by a lender as independent contractors are permitted to be registered through Technology Manager as authorized users of the lender. However, individuals who are employees of third party contracting firms that are used by a lender for outsource services such as contract underwriting, pipeline management or asset management ("mortgage service providers"), regardless if the services are provided onsite at the lender's shop, may not be registered as authorized users of the lender. Contact your Technology Account Manager if any mortgage service providers need access to Fannie Mae technologies.

Data Access Authorization Reminders

Lenders are reminded that a Data Access Authorization Agreement is required in order for a mortgage service provider to be given access to the lender's data via a Fannie Mae technology application. Additionally, mortgage service providers accessing a lender's data via a Fannie Mae technology application must be licensed to use the technology application under their own Fannie Mae Software Subscription Agreement (and, except in some limited circumstances, must obtain user IDs and passwords through their own Technology Manager account). Consult your Technology Account Manager for assistance.

Technology Application Password Tips

It is a recommended best practice that organizations elect Fannie Mae's password expiration option for user IDs associated with Fannie Mae technology applications in order to facilitate the 90-day user password resets required in the Software Subscription Agreement.

Why is it important to implement password expiration?

Effective password management practices reduce the risk of unauthorized users gaining access to critical company systems and data. We integrate a number of security controls in our technology applications to help ensure that access is restricted to authenticated users. One such security control – password expiration – is offered as a recommended layer of security protection.

For whom should you implement password expiration?

Password expiration should be implemented for all user IDs, except for certain situations like:

- System IDs used for integration purposes are exempt from the 90-day password reset requirement; however, in accordance with the Software Subscription Agreement, passwords should be reset annually for these System IDs.
- User IDs and passwords are embedded or hidden from the user.

How do you implement password expiration for your Fannie Mae technology?

Corporate Administrators within Technology Manager can edit their company configuration within Technology Manager directly. Use job aids available within the tool to guide you through password management options.

More information on Technology Manager for Administrators, to include training resources and job aids, can be found on fanniemae.com:

Technology Manager for Single-Family Lenders

Technology Manager for Multifamily Lenders

> NOTE: *This summary is intended for reference only. All criteria are subject to the formal terms and conditions of the Fannie Mae Selling Guide. In the event of any conflict with this document, the Selling Guide will govern. For more information, visit FannieMae.com.*

Questions?

For further assistance, call the Customer Interaction Center at 800-2FANNIE. Enter your user ID when prompted and select silent option 8 at any time. Option 8 will not be announced as a menu option because it is only for administrators. For more information, please contact your Fannie Mae representative.