UWM®
UNITED WHOLESALE MORTGAGE

# PASSPHRASE (PASSWORD) POLICY CHANGE

## OVERVIEW

UWM has implemented a new passphrase policy effective immediately for all team members. A passphrase is similar to a password in usage, but is generally longer for added security. This job aid includes details on the new policy and reminders of how to create strong passphrases.

- **PASSWORD** – is constructed of a random combination of special characters, letters, and numbers with variable lengths.
  - Example: L28sB%9R4
- **PASSPHRASE** – is constructed of a series of words or phrases totaling at least 12 characters without spaces. The series of words or phrases make the passphrase easier to remember and more secure.
  - Example: $implicityYardRed7

## POLICY CHANGE

This policy update will affect the number of characters required for a passphrase as well as the cadence of how often team members need to update their passphrases.

The process to update passphrases will not change with the new policy. Team members will still receive reminder emails 14 days before their passphrase expires.

See the section below for details on the new requirements for passphrases at UWM.

### UPDATED REQUIREMENTS FOR STANDARD ACCOUNTS

- Passphrase must be a minimum of 12 characters
- Passphrase must be updated every 12 months
- CANNOT reuse the last 24 passphrases

**NOTE**: Team members still have 6 attempts to enter a correct passphrase before being locked out. Once locked out, team members will need to contact the Service Desk to verify and reset the passphrase or retry after 30 minutes.

### UPDATED REQUIREMENTS FOR SPECIAL ACCOUNTS

While most team members at UWM will fall under the standard account requirements, a few other account types have stricter passphrase requirements. See the table on the following page to review the differences among the account types and their passphrase requirements.

## NEW PASSPHRASE POLICY REQUIREMENTS PER ACCOUNT TYPE

| | STANDARD ACCOUNTS | SHARED TEST ACCOUNTS | ELEVATED ACCOUNTS | SERVICE ACCOUNTS |
|---|---|---|---|---|
| **MINIMUM LENGTH** | 12 Characters* | 12 Characters* | 16 Characters* | 32 Characters* |
| **PASSPHRASE HISTORY** | Last 24 | Last 24 | Last 24 | Last 24 |
| **PASSPHRASE COMPLEXITY** | None* | None* | None* | None* |
| **MINIMUM AGE** | 1 Day | None | 1 Day | 1 Day |
| **MAXIMUM AGE (EXPIRATION)** | 1 Year* | 12 Hours | 1 Year* | 1 Year |
| **LOCKOUT POLICY** | 6 Attempts | 6 Attempts | 6 Attempts | 6 Attempts |
| **UNLOCK POLICY** | 30 Minutes* | 30 Minutes* | Admin Action | Admin Action |
| **COMMON WORDS** | Disallowed | Disallowed | Disallowed | Disallowed |

* New requirements

## CREATING STRONG PASSPHRASES

UWM's new passphrase policy encourages team members to use strong, secure passphrases.

Below you will find dos and don'ts for creating a strong passphrase:

### TIPS FOR CREATING STRONG PASSPHRASES

- Use a mixture of capital letters, numbers, and special characters (!@#$%^&*)
  - Example:
    - Duckpencild0nutfork! (Duck pencil donut fork!)
- Use a phrase and incorporate shortcut text or acronyms
  - Example:
    - 4Score&7yrsAgo (Four score and seven years ago)
- Use common elements but customized to specific sites
  - Examples:
    - Bank Passphrase – Pwrd4acct-$$
    - Netflix Passphrase – Pwrd4Ntflx_Wa7ch

### THINGS TO AVOID

- Do not include your or your family's personal information such as birth month/day, pet names, addresses, etc
- Do not use sequential numbers (1234) or sequential keys on the keyboard (asdf)
- Do not use a single word even if it meets the length requirements
- Do not use the same passphrases for multiple accounts

**If you have any questions or concerns,<br>please reach out to Service Desk by submitting a ticket to YouSupport or call x4500.**