APPLICATION SECURITY SETTINGS MANUAL

March 2024

Document Revision History

Document Version	Created By	Revision Date	Modification Details
Version 1.0	Olatayo Adeoye	N/A	Document Created

N/A: Not applicable

Application Security Settings Manual

This manual seeks to provide developers/development team information on the approved security configurations that are expected on all applications developed for FMDQ.

1. Password Policy/Settings

Password setting refers to the process of creating a password for a user account. A strong password typically consists of a combination of uppercase and lowercase letters, numbers, and special characters. Below are the password settings expected on applications developed for FMDQ use:

- Default password change shall be enforced on first login by user on all applications
- Passwords must be renewed after thirty (30) days of usage
- System shall prevent user from reusing same password until after ten (10) renewals
- The systems must use an irreversible encryption method for storing passwords
- All passwords shall follow the password construction guidelines provided below. Strong passwords have the following characteristics:
    a. Contain at least 8 alphanumeric characters
    b. Contain both upper- and lower-case letters
    c. Contain at least one number (for example, 0-9)
    d. Contain at least one special character for example: ,!$%^&*()_+|~-=\`{}[]:";'<>?/.
    e. Can be up to 128 characters long

2. Session Management and Lockout

To prevent Session Hijacking and Brute Force attacks from occurring to an active session, the HTTP server is expected to seamlessly expire and regenerate tokens to give an attacker a smaller window of time for replay exploitation of each legitimate token: The following policies shall apply:

- Account lockout shall be set to activate when there is no activity for a period not more than five (5) minutes
- Whenever wrong passwords are provided, accounts shall be locked out after three (3) consecutive, unsuccessful attempts