REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF INTERNAL REVENUE

January 5, 2024

REVENUE MEMORANDUM ORDER NO. 5-2024

Subject **POLICIES AND PROCEDURES FOR THE IMPLEMENTATION OF MULTI-FACTOR AUTHENTICATION (MFA) FOR VIRTUAL PRIVATE NETWORK (VPN) ACCESS**

To **ALL INTERNAL REVENUE OFFICIALS, EMPLOYEES, AND OTHERS CONCERNED**

---

1. BACKGROUND

With the advancement of technology, cyber threats have also evolved. The need to protect access to the BIR's critical systems, sensitive data and privileged accounts are some of the reasons why the Bureau is implementing the Multi-Factor authentication.

Multi-Factor Authentication (MFA) is a stronger authentication method to enhance security by requiring a user to provide two or more verification factors before gaining access to a BIR resource. Through MFA a user will be required to identify themselves by more than a username and password thus reducing the risk of unauthorized access in case passwords are compromised. All VPN users with access to BIR systems shall be authenticated using two or more verification factor before gaining access to BIR resources.

This Order provides clear-cut policies and procedures for the use of Multi-Factor Authentication (MFA) when accessing the BIR network thru Virtual Private Network (VPN).

2. OBJECTIVE

To strengthen the security control in place when accessing application system by implementing a stronger authentication method on Bureau's VPN.

3. DEFINITION OF TERMS

- **Authentication** refers to the identification requirements associated with an individual using a computer system. Identification information must be securely maintained by the computer system as it can be associated with an individual's authorization and system activities. Three types of factors are used to provide authentication: a) something you know (e.g., a password) b) something you have (e.g., a certificate or smart card) c) something you are (e.g., a fingerprint or retinal pattern).
- **Multi-Factor Authentication (MFA)** refers to an authentication method that requires a user to provide at least two factors of verification in order to be granted access to a website, application or resource.

- **Virtual Private Network (VPN)** refers to a method of providing secure remote access when accessing BIR resources.
- **VPN User** refers to a BIR user/Contractors with remote access to a BIR resource.
- **Server Network Access Request Form (SNARF)** refers to a request form being filled out by a user when requesting access on BIR network.
- **One-Time Password (OTP)** refers to a one-time pin, one-time authorization code or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device.
- **User Interface (UI)** refers to a point of human-computer interaction and communication in a device. This can include display screens, keyboards, a mouse and the appearance of a desktop.
- **User Portal** refers to a webpage where users can create an account, change their personal information, and choose a two-factor authentication method.

4. POLICIES

4.1 MFA shall be required for all users of the Bureau's VPN.
4.2 VPN users shall be responsible for all activities identified with the account.
4.3 One-time password/pin shall be generated using a mobile application or sent through the registered BIR email address.
4.4 VPN users with existing access or requesting for new access (both BIR employees and third party service providers) shall accomplish two (2) copies of SNARF (see Annex A) with appropriate Network Diagram attached.
4.5 Accomplished/Signed SNARF with appropriate Network Diagram shall be submitted to Security Management Division (SMD). Other necessary documents maybe required upon evaluation, if needed (e.g. NDA (3rd party), Justification letter, etc.). VPN access request shall only be evaluated by SMD upon submission of complete documentary requirements.
4.8 Account locked out shall be imposed after a maximum of three (3) consecutive invalid log in attempts. User with locked account or forgotten password shall be logged in BIR Service Desk System for unlocking of account or resetting of password.
4.9 Any issue or difficulties encountered associated with the use/enrollment of MFA shall be reported to SMD.

5 PROCEDURES

5.1 The VPN requestor/user shall:
5.1.1 Accomplish the SNARF.
5.1.2 Forward the duly accomplished two (2) copies of form with corresponding attachment to the Head of Office/Project Manager for approval.
5.1.3 Receive thru email the vulnerabilities that needs to be addressed, if any.
5.1.3.1 Remediate vulnerabilities found.
5.1.3.2 Inform SMD of the remediation done and request to repeat conduct of Vulnerability Assessment (VA).
5.1.4 Receive thru email the login/password for VPN and MFA.
5.1.5 Proceed with their individual account creation on the MFA User Portal following the step-by-step procedure on the email notification sent by SMD.

5.2 The Head of Office/Project Manager shall:
5.2.1 Evaluate and sign the accomplished request form (beside signature of requesting party).

5.2.2 Endorse the request form and corresponding attachment to SMD.

5.3 SMD Security Analyst shall:

5.3.1 Receive the request forms with corresponding attachment and review/evaluate the SNARF with regard to information accuracy and completeness.

5.3.1.1 Perform Vulnerability Assessment (VA) to the Desktop/Laptop of the VPN user, if needed.

5.3.1.1.1 If found to have vulnerabilities, email VPN user with the findings.

5.3.1.1.2 Reconduct VA after remediation/fixes have been applied by the VPN user.

5.3.2 Process the SNARF within one (1) working day from evaluation and/or reconduct of VA and endorse request to SMD Chief for approval.

5.3.3 Endorse the SNARF and corresponding attachment to concerned offices:

5.3.3.1 System Administrator (Sys Ad) from Data Warehousing and Systems Operations Division (DWSOD) for evaluation and affix their initial/signature to the form.

5.3.3.2 DWSOD Sys Ad shall transmit the signed SNARF within one (1) working day from evaluation to Network Administrator (Net Ad) Network Management and Technical Support Division (NMTSD) after their initial/signature.

5.3.3.3 NMTSD Net Ad shall evaluate the SNARF and affix their initial/signature to the form.

5.3.3.4 NMTSD Net Ad shall transmit the signed SNARF within one (1) working day from evaluation to Office of the ACIR-Information Systems Development and Operations Service (ISDOS) for final approval.

5.3.3.5 ACIR-ISDOS shall evaluate the SNARF and affix their signature to the form as the final approver.

5.3.3.6 Upon approval, OACIR-ISDOS shall transmit signed SNARF within one (1) working day from evaluation to SMD.

5.3.3.7 SMD shall transmit approved SNARF and corresponding attachment to NMTSD Net Ad for implementation of VPN request within one (1) working day from receipt of approved SNARF.

5.3.3.8 NMTSD Net Ad shall implement request within twenty-four (24) hours upon receipt of approved SNARF.

5.3.3.9 NMTSD Net Ad shall notify VPN user through email of his/her login credentials.

5.3.4 Enroll VPN user/requestor with approved SNARF on the MFA Management UI.

5.3.5 Notify VPN user through email of his/her MFA login credential and the procedure for account enrollment on MFA User Portal.

5.4 The DWSOD Sys Ad shall:

5.4.1 Receive the SNARF and evaluate request.

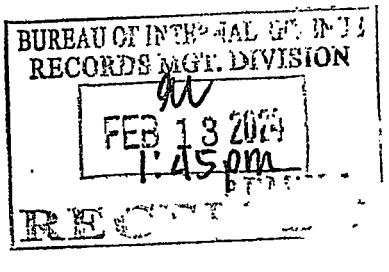
5.4.2 Endorse the SNARF to DWSOD Chief for approval.

5.4.3 Route the SNARF to NMTSD.

5.5 The NMTSD Net Ad shall:

5.5.1 Receive the SNARF and evaluate request.

5.5.2 Endorse the SNARF to NMTSD Chief for approval.



5.5.3 Route the SNARF to OACIR-ISDOS for final approval.
5.5.4 Email the VPN login credentials to requesting user.

5.6 The ACIR-ISDOS shall:
5.6.1 Receive the SNARF and evaluate request.
5.6.2 Sign the SNARF as the final approver.
5.6.3 Route the approved SNARF to SMD for endorsement to NMTSD for implementation.

6 REPEALING CLAUSE

All other issuances and/or portions thereof inconsistent herewith are hereby revoked and/or amended accordingly.

7 EFFECTIVITY

This Order takes effect immediately.

ROMEO D. LUMAGUI, JR.
Commissioner of Internal Revenue

BUREAU OF INTERNAL REVENUE
RECORDS MGT. DIVISION
FEB 13 2024
1:45pm
RECEIVED