Bringing In Revenues
for Nation-Building

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF INTERNAL REVENUE

Quezon City

BAGONG PILIPINAS

April 14, 2025

REVENUE MEMORANDUM ORDER NO. 024-2025

Subject **IMPLEMENTATION OF BRING YOUR OWN DEVICE (BYOD)**

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

I. BACKGROUND

With the rapid advancement of mobile technology and the growing demand for flexible work environments, the BIR will implement BYOD strategy to allow employees and other authorized third parties (partner, consultant, and contractor / service provider) to use their personal devices for work-related activities offering more convenience, flexibility, and productivity. This approach can improve the satisfaction of employees and other parties allowed to use personal device/s by enabling the use of said devices. However, implementing BYOD also introduces challenges related to data security, privacy and compliance. To address these, BYOD policies and guidelines are hereby prescribed to ensure secure and effective integration into the BIR workplace.

II. OBJECTIVE

This Order is issued to:

a. Ensure security, confidentiality and integrity of information when accessing BIR network through personal device/s;

b. Prescribe policies, guidelines and procedures on the implementation and use of personal device/s.

III. POLICIES AND GUIDELINES

A. The following persons shall be allowed to use personal device/s:

- Employees
- Consultant/Contractor/Service Provider
- Partner government agencies, and
- Other Third Parties except those accessing BIR network for one-day presentation purposes only

The following personal device/s shall be allowed to be connected to the BIR network/resources:

1. Laptop
2. Smartphone/tablet
3. Desktop Computer
4. Printer (applicable only if allocation of printer by Property Division is insufficient)

BUREAU OF INTERNAL REVENUE
RECORDS MANAGEMENT DIVISION
RECEIVED
MAY 07 2025
ADMIN UNIT - 1
BY: TIME: 9:50

C. BYOD Users shall strictly:

1. Abide by the Policies and Guidelines on Revised Information and Communications Technology (ICT) Security Policy (RMO 15-2014) and Republic Act 10173 (Data Privacy Act of 2012).
2. Adhere to the Acceptable Use Policy (AUP).
3. Undergo Information Security Awareness and Data Privacy Act briefings in order to register and use their personal devices (applicable only to BIR employees and contractors).
4. Users who need to connect their personal device/s to the BIR's internet shall register first their devices and comply to this issuance before requesting and be given access to the internet using their personal devices.
5. Allow authorized ISG personnel to access/inspect registered personal device/s, including conduct of vulnerability assessment (VA). However, *employees accessing BIR network (WiFi) using smartphone/tablet shall not undergo VA.*
6. Ensure that:
   - 6.1 updates are regularly applied to the operating system and primary applications such as email client, web browser and security software. Updates shall be the responsibility of the user.
   - 6.2 personal and BIR-related files/application systems are encrypted and separated from one another (i.e. a dedicated folder/storage used as a repository for official/work related files and/or application systems)
7. Secure the device/s to prevent sensitive data from being loss or compromised. Be fully liable for the loss of BIR data stored therein. BIR shall not be responsible for the loss of the registered device/s.
8. Report to authorized BIR personnel lost or stolen device/s within 24 hours.
9. Handle other issues not related to BIR network/resources.
10. Ensure removal/deletion of work-related data prior to disposal/pullout of the registered device.

D. Personal device/s to be connected to the BIR network/resources of:

1. Third party/guest shall:
   - 1.1 be limited to a single device access.
   - 1.2 be allowed for one-day connectivity if purpose of connection is for presentation only.
   - 1.3 be disconnected from the network in case of anomaly or suspicious activity without prior notice.
2. BIR employees and All Other Users shall:
   - 2.1 be registered with BIR by accomplishing BYOD application form except for those requesting for one-day connectivity and for presentation purposes only.
   - 2.2 be limited to a single device access; further, BIR officials (holding director item/position) shall be allowed access to three (3) devices
   - 2.3 undergo vulnerability assessment (VA) for laptops/Desktop PC.
   - 2.4 have an advance endpoint security solution (e.g. Malwarebytes, eScan) and activated the following security features of the device:
     - a. password/Personal Identification Number (PIN)/biometrics protection
     - b. encryption of data stored therein (e.g bitlocker)

BUREAU OF INTERNAL REVENUE
RECORDS MANAGEMENT DIVISION
RECEIVED
MAY 07 2025
ADMIN UNIT-2
BY: TIME: 9:50

2.5 be allowed only for a maximum of three (3) months network connection.

2.6 be subjected to the following, once approved:

2.6.1 installation of Endpoint Detection and Response (EDR) agent/solution.

2.6.2 regular onsite inspection and/or post audit by authorized Revenue Data Center (RDC)/Network Management and Technical Support Division (NMTSD) technical support personnel.

2.6.3 be disconnected from the network in case of anomaly or suspicious activity without prior notice.

E. Application to use the Personal Device and Conduct of VA

1. Application Form for BYOD, AUP and submission of certificate of attendance to the Information Security Awareness and Data Privacy Act Briefing shall be digitally submitted by the requestor by accessing the QR code or link as provided on a separate memorandum.
2. Conduct of VA shall be done by Security Management Division (SMD), RDC technical support personnel or Regional Tech support personnel.
3. Approval/Disapproval of BYOD application is done thru the workflow, included in the MS Forms submitted by requestor.

IV. ROLES AND RESPONSIBILITIES

A. User/Requestor

1. Access the *QR Code/Link* for request of more than one (1) day connectivity; otherwise create a ticket on Servicedesk thru coordination with the point person from BIR for 1 day connectivity for presentation purposes only.
2. Fill-up the online forms and upload the Certificate of Attendance to the Information Security Awareness and Data Privacy Act Briefing (applicable only to BIR employees and contractors).
3. Resolve vulnerabilities found in the device, if any. Provide additional requirement as may be required (applicable to laptop/desktop PC).
4. Receive email notification on the status of BYOD application.

B. RDC-CONED / NODC-CONED/NMTSD

1. Receive email notification of user's request for BYOD of more than one (1) day connectivity; otherwise receive email notification from Servicedesk for request valid for 1 day connectivity.
2. Validate completeness and accuracy of request.
3. Evaluate the request as to the:
   a. reason/justification for the request
   b. inventory of desktop computers/printers provided to their office,
   c. conformance of the device/s to the security features requirement including the advance endpoint security solution

BUREAU OF INTERNAL REVENUE
RECORDS MANAGEMENT DIVISION
RECEIVED
MAY 07 2025
ADMIN UNIT - 1
BY: TIME: 9:50

4. Conduct vulnerability assessment (VA) if the device is laptop or desktop PC (applicable to RDC-CONED/NODC-CONED only).
   a. If with vulnerabilities, inform and/or assist user/requestor on the resolution of vulnerabilities.
   b. Re-conduct VA if vulnerabilities have been resolved.
5. Approve request if it pass the evaluation, otherwise, disapprove the request.
6. Implement connection of the device to the BIR network if approved by the RDC Head/NMTSD Chief.
7. Provide assistance to SMD on the installation of EDR
8. Prepare the following monthly inventory list and submit to Office of ACIR-ISDOS/SMD:
   a. approved/disapproved registration for BYOD from the list of requests generated thru Sharepoint.
   b. list of disconnected devices from the network (if any).
9. Conduct quarterly onsite inspection and/or post audit of the registered devices for BYOD to offices under their area of jurisdiction.
10. Prepare onsite inspection / post audit report and submit to OACIR-ISDOS, copy furnish SMD.

C. NMTSD

1. Endorse BYOD request from National Office (N.O) to SMD thru email for conduct of VA.
2. Receive notification from SMD of the vulnerabilities found, (if any) for laptop/desktop PC BYOD request.
3. Inform SMD if vulnerabilities have been resolved for re-conduct of VA.
4. Monitor approved devices connected to the BIR network.
5. Work closely with concerned offices on security breaches relative to the use of BYOD.
6. Coordinate with SMD on security matters relative to BYOD Policy.
7. Analyze and implement required mitigation on identified security breaches.

D. SMD

1. Receive thru email-the endorsed N.O request/s from NMTSD for conduct of VA.
2. Conduct VA on laptop/desktop PC.
3. If with vulnerabilities, inform NMTSD of the vulnerabilities for resolution.
4. Re-conduct VA if vulnerabilities have been resolved.
5. Inform NMTSD thru email if laptop/desktop has been cleared from VA.
6. Install EDR agent/solution to the approved device.
7. Receive from RDC-CONED/NODC-CONED/NMTSD the monthly inventory list of the approved/disapproved registration for BYOD.
8. Receive from RDC-CONED/NODC-CONED/NMTSD the onsite inspection/post audit report.
9. Monitor approved BYOD connected to the BIR network.
10. Work closely with concerned offices on security breaches relative to the use of BYOD.
11. Analyze and implement required mitigation on identified security breaches.

BUREAU OF INTERNAL REVENUE
RECORDS MANAGEMENT DIVISION
RECEIVED
MAY 07 2025
BY: ________ TIME: 9:20

F. OACIR-ISDOS

1. Receive from RDC-CONED/ NODC-CONED/NMTSD the monthly inventory list of the approved/disapproved registration for BYOD and the list of disconnected devices from the network (if any).
2. Receive from RDC-CONED/NODC-CONED/NMTSD the onsite inspection/post audit report.
3. Review submitted inventory list/post audit report and provide recommendation or necessary corrective action to concerned office, if applicable.

V. EFFECTIVITY

This Order shall take effect immediately.

ROMEO D. LUMAGUI, JR.
Commissioner of Internal Revenue

BUREAU OF INTERNAL REVENUE
RECORDS MANAGEMENT DIVISION
RECEIVED
MAY 07 2025
ADMIN UNIT - 1
BY: TIME: 7:50