REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF INTERNAL REVENUE

Bringing In Revenues
for Nation-Building

BAGONG PILIPINAS

January 31, 2025

REVENUE MEMORANDUM ORDER NO. 010-2025

Subject **POLICIES AND GUIDELINES ON THE USE OF BIR INTERNET BROWSING FACILITIES**

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

I. OBJECTIVE

This Order prescribes the policies, guidelines and procedures on the implementation and use of BIR internet service by authorized users to prevent misuse, ensure confidentiality and protection of data, maintain productivity, and safeguard the agency's reputation.

II. POLICIES AND GUIDELINES

2.1. BIR internet services shall strictly be for official use only.

2.2. Internet users shall be mindful of their online activities and ensure responsible and productive use of BIR internet facility

2.3. Users shall undergo Information Security Awareness Briefing (ISAB) prior to internet access processing and approval.

2.4. Granting of Internet Access

2.4.1 Internet services shall be granted based on the user's role/current job description.

2.4.1.1 Use and access of *wired internet* account shall be granted but not limited to the following users:

2.4.1.1.1 Officials/Employees with Webmail license

2.4.1.1.2 Officials/Employees required to perform on-line system related activities

2.4.1.1.3 Officials/Employees with constant research activities

2.4.1.1.4 Officials/Employees involved in inter-agency projects approved by Assistant Commissioner of Information Systems Development and Operations Service (ACIR ISDOS) or Deputy Commissioner of Information Systems Group (DCIR ISG).

2.4.1.1.5 Other employees and third parties within the BIR organization recommended by Head of Office and

BUREAU OF INTERNAL REVENUE
RECORDS MANAGEMENT DIVISION
RECEIVED
MAR 04 2025
BY: ADMIN UNIT - 1 TIME: 1:40pm

approved by ACIR ISDOS or DCIR ISG.

2.4.1.2 Use and access of *wireless internet* account shall be granted but not limited to the following users:

2.4.1.2.1 Officials/Employees with BIR issued laptop

2.4.1.2.2 Officials/Employees involved in inter-agency projects endorsed by ACIR ISDOS and approved by DCIR ISG

2.4.1.2.3 Guest/External Users

2.4.2 BIR Officials and select employees with webmail, performing online system related activities, and constant research activities shall automatically be given privilege to access the internet upon submission of duly accomplished BIR Form No. 0041-Office Automation Request (Annex A) to Network Management and Technical Support Division (NMTSD).

2.4.3 User requesting for *wired internet access* shall submit duly accomplished Annex A to Chief, NMTSD for endorsement / recommendation for approval of ACIR ISDOS.

2.4.4 User requesting for *wireless internet access* for BIR issued equipment shall log a ticket thru Service Desk for internet account activation and configuration upon approval of ACIR ISDOS.

2.4.5 User requesting for wireless internet access for their personal device/s shall comply first to the policy on the implementation of Bring Your Own Device (BYOD) before given the privilege to access the internet.

2.4.6 In case of transfer to another office, users with approved wired/wireless internet access shall request for reactivation by submitting a duly accomplished Annex A to Chief, NMTSD.

2.5. The internet administrator shall keep an updated inventory of all internet users/access.

2.6. All internet activities are being monitored and subject to inspection and/or sanction in case of violation.

2.7. Resource Usage

2.7.1 All users shall follow the Bureau principles regarding resource usage and exercise good judgment in using internet services.

2.7.2 Acceptable use of the internet for performing job functions may include, but not limited to:

2.7.2.1 Downloading of software upgrades and patches by Systems Administrators and other authorized users;
2.7.2.2 Review of possible vendor web sites for product information;
2.7.2.3 Research or reference for regulatory and technical information;
2.7.2.4 Use of Voice over internet Protocol (VoIP) and
2.7.2.5 Accessing of personal email account.

2.7.3 Acceptable use of the internet for guest/external user may include, but not limited to:
2.7.3.1 Accessing BIR eServices and other government agencies services
2.7.3.2 Research for tax related information
2.7.3.3 Accessing personal email account

2.8. Prohibition

2.8.1 Acquisition, storage, and dissemination of data through the internet which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically and strictly prohibited;
2.8.2 The Bureau also prohibits the conduct of a personal or private business enterprise, political activity, engaging in any form of intelligence collection from Bureau facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials;
2.8.3 Automatic updating of software or information on the Bureau's information assets via background "push" internet technology are prohibited, unless the involved vendor's system has first been tested and approved by the NMTSD;
2.8.4 Downloading files directly into a network server or production machine from untrusted or unauthorized sources is prohibited;
2.8.5 Employees or individual offices are prohibited from creating websites, blogs, forums and other internet offerings containing the Bureau information independent of the Bureau official web infrastructure unless otherwise duly authorized/approved by the Bureau Management;
2.8.6 Other specific activities that are strictly prohibited include but are not limited to:
2.8.6.1 Accessing information that is not within the scope of one's work (e.g., unauthorized access of personnel file information, accessing information that is not needed for the proper execution of job functions);
2.8.6.2 Misusing, disclosing without proper authorization, or altering personnel information (e.g., making unauthorized changes to a personnel file, or sharing electronic personnel data with unauthorized personnel);
2.8.6.3 Any unauthorized, deliberate action that damages or may cause damages or disrupts computing systems or networks, alters their normal performance, or causes them to malfunction regardless of location or duration;
2.8.6.3.1 Perpetrate any form of fraud, and/or software, film or music piracy;

2.8.6.3.2 Hacking activities;

2.8.6.3.3 Willful or negligent introduction of computer viruses, Trojan or other destructive programs into Bureau systems or networks or into external systems and networks;

2.8.6.3.4 Unauthorized decryption or attempt at decryption of any system or user passwords or any other user's encrypted files;

2.8.6.3.5 Packet sniffing, packet spoofing, or use of any other means to gain unauthorized access to a computing system or network;

2.8.6.3.6 Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization;

2.8.6.3.7 Downloading of any shareware or freeware programs or files;

2.8.6.3.8 Any conduct that constitutes or encourages a criminal offense, leads to civil liability, or otherwise violates any national or international laws, and regulations;

2.8.6.3.9 Deliberate pointing or hyper linking of Bureau Websites to other internet sites whose content may be inconsistent with or in violation of the aims or policies of the Bureau;

2.8.6.3.10 Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls;

2.8.6.3.11 Browsing, creating, posting, transmitting, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, gambling, anti-religion, violence, racism or political beliefs;

2.8.6.3.12 Unauthorized ordering (shopping) of items or services on the internet;

2.8.6.3.13 Online gambling and gaming through the internet;

2.8.6.3.14 Unauthorized subscription to mailing list or mail services;

2.8.6.3.15 Unauthorized participation in any online contest, online business or promotion;

2.8.6.3.16 In no case shall social networking sites (e.g., Pinterest, Tagged, Tumblr, LinkedIn), instant messaging tool (e.g. Yahoo Messenger, FB Messenger, Gtalk) and file sharing sites (e.g., Limewire, Bittorent, Mediafire) be allowed for access over the internet except for authorized officials/employees and

BUREAU OF INTERNAL REVENUE
RECORDS MANAGEMENT DIVISION
RECEIVED
MAR 04 2025
BY: ADMIN UNIT - 1 TIME 1:40pm

2.8.6.3.17 All other analogous acts.

2.8.7 Automatic scanning for virus shall be installed on all PCs and servers accessing the internet and shall not be turned off by the user or the System Administrator;

2.8.8 All PCs, servers, and other network components shall comply with guidelines on the prevention, detection, and removal of computer viruses, worms, trojan, and other forms of malicious programs.

2.9. Anti-malware Protection

2.9.1 All authorized software downloaded from non-Bureau sources through the internet shall be screened with virus detection and protection software before installation;

2.10. Maintaining Organization's Image

2.10.1 Whenever employees state an affiliation to the Bureau, they shall also clearly indicate that the opinions expressed are their own and not necessarily those of the Bureau.

III. ROLES AND RESPONSIBILITIES

3.1. **Requester/User (BIR employees/third party personnel) shall:**

3.1.1. Submit duly accomplished BIR Form No. 0041-Office Automation Request (Annex A) and duly signed by concerned Head of office to NMTSD.

3.1.2. Request reactivation of internet access in case of office transfer by submitting a duly accomplished Annex A to NMTSD.

3.2. **Concerned Head of Office shall:**

3.2.1 Recommend approval of wired/wireless internet access request/s of BIR employees/third party personnel.

3.3. **Network Management and Technical Support Division (NMTSD) shall:**

3.3.1 Validate and recommend approval of internet access requests of BIR employees and third party personnel to ACIR ISDOS

3.3.2 Grant approved wired/wireless internet access request/s

3.3.3 Approve automatic updating of software or information on the Bureau's information assets via background "push" internet technology and

3.3.4 Administer proxy server/s, firewall architecture, and other network systems as far as internet access and internet security are concerned as well as maintain its documentation and configuration details.

3.3.5 Maintain an up-to-date record of all users with internet access.

3.3.6 Monitor internet usage, bandwidth consumption, download/upload speeds, access time, potential security threats thru network monitoring tools;

3.4. **Assistant Commissioner – ISDOS (ACIR-ISDOS) shall:**

3.4.1 Approve/Disapprove wired/wireless internet access requests of BIR employees and third party personnel endorsed by NMTSD;

3.4.2 Endorse/Recommend approval of wired/wireless internet access request/s to the Deputy Commissioner, Information Systems Group, as necessary.

3.5. **Deputy Commissioner – ISG shall:**

3.5.1 Approve/Disapprove wired/wireless internet access request/s endorsed by ACIR-ISDOS as necessary.

IV. SANCTIONS

Non-compliance with the Internet Security Guidelines shall be subject to immediate disciplinary and/or legal actions based on RMO 67-2010 Policies & Guidelines on Information & Communication Technology Security Offense.

V. REPEALING CLAUSE

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

VI. EFFECTIVITY

This Order shall take effect immediately.

ROMEO D. LUMAGUI, JR.
Commissioner of Internal Revenue

G-4

BUREAU OF INTERNAL REVENUE
RECORDS MANAGEMENT DIVISION
RECEIVED
MAR 04 2025
BY ADMIN UNIT - 1 TIME: 1:40pm