Policies and Standards on the Use of the Computer, Network and other Technology Resources

This policy applies to all activities that involve the use of the Bureau of Internal Revenue's (BIR) information systems, computing equipment, PCs, peripherals, information media and communications infrastructure. This includes, but is not limited to, hardware, software, database and server access, and network communications including Internet connectivity.

This policy also applies to all external communications via E-mail, social networking, or other electronic media which relate to the BIR's transactions or involve the BIR's resources – whether the communications' forum or medium is the public Internet or any other similar medium.

1. Computer and Network Infrastructure Use

1.1. Accountability

1.1.1. The computers are assigned to individual users who are accountable for their maintenance and upkeep.

1.1.2. Users will be fully liable for the loss of the computer unit, including its accessories/peripherals, regardless of when, where or how the loss occurs.

1.1.3. Users shall ensure the protection of the computer unit and all information stored in it.

1.2. Usage

1.2.1. The BIR's information systems (computers, servers, systems and networks) shall be used for official and authorized purposes only.

1.2.2. Tampering or making unauthorized modifications to the BIR standard operating system configuration is strictly prohibited.

1.2.3. Multiple simultaneous sessions of two users in one terminal is not allowed. Users must log off a terminal that has an active log-on session connected to it whenever leaving and/or once another user logs in the same terminal.

1.2.4. Users must log-in on the terminal located on their assigned office or division only. Written approval from SMD must be obtained should there be a business need for the user to log in from a terminal located in a different office or division.

1.2.5. For security purposes, all user activities may be monitored by authorized personnel to ensure and preserve the functionality and integrity of the BIR's computer systems and facilities.

1.2.6. Unless authorized, bringing in and using personal, non-BIR issued computers (even stand-alone use) inside the office is not allowed.

1.2.7. Users are responsible for ensuring that the latest antivirus definitions and necessary patches, security updates and service packs are installed on the computer. Users are required to connect their workstations and log-in to the network in order to receive the necessary updates.

1.2.8. Installation and use of illegal, unauthorized or unlicensed software copies on BIR computers are strictly prohibited.

1.2.9. Only BIR issued networking devices and equipment are to be used in the office. Personal networking devices (switches and hubs, etc.) are not allowed.

1.2.10. Only BIR issued, supported and/or managed wireless access point must be used.

1.2.11. The following are considered policy violations or non-business related use of the BIR's resources:

- Use of excessive network bandwidth that affects network performance and access to network resources

- Download, storage, reproduction and distribution of the following, but not limited to, copyrighted music and/or movies (audio, video, MP3, MPEG and other multimedia formats), games, pornographic and sexually explicit materials through local drives and network shares
- Installation and use of unlicensed software that violates applicable software licensing agreements or copyright laws
- Use of applications and other methods that circumvent or bypass network security, firewall and proxy restrictions
- Unauthorized sending of network broadcast messages.

2. Accounts and Passwords

2.1. Accounts, passwords and other types of authorization that are assigned to individual users should not be shared with others for any reason. Users are responsible for all activities identified with the account.

2.2. Passwords must comply with the BIR's guidelines thereon such as, but not limited to:

2.2.1. At least 8 alphanumeric characters

2.2.2. Passwords must be changed every 90 days, or when confidentiality has been breached

2.2.3. Last 5 passwords must not be used

2.2.4. Maximum of 3 consecutive invalid login attempts

2.3. Passwords must not be written down in some easily readable form (post-it notes) and left in a place where unauthorized persons might see them.

3. Internet Access and E-mail

The E-mail facility, including all related Bureau computers and network resources, are intended for official BIR purposes only.

3.1. E-mail Facility

3.1.1. Users shall use only the BIR's official E-mail system in sending confidential and sensitive information.

3.1.2. Users are to refrain from sending unsolicited E-mail messages, such as SPAM, which includes the sending of "junk mail" and/or other advertisements sent to individuals who have not requested such materials.

3.1.3. E-mail messages should be prepared with the same degree of care, judgment and discretion as in all other forms of written official communications.

3.1.4. Confidential files must not be sent thru E-mail unless encrypted.

3.1.5. Files should be scanned for viruses and other malicious software before being attached and sent.

3.1.6. Users should manage file attachments and regularly delete old and unneeded E-mails to maintain their database size within limit.

3.1.7. Attachments from unknown or unsecure sources must not be opened. All e-mail attachments, regardless of the source or content, must be scanned for viruses and other destructive programs before being opened or stored on any of the BIR's information system.

3.1.8. Users should not use an E-mail account assigned to another individual to either send or receive messages.

3.2. Internet Access

3.2.1. Only web sites that are applicable to the user's line of work may be accessed. Websites that fall under the following categories, but not limited to, Anonymizer, Games, Audio, Videos, Gambling, Nudity and Sex, Social and Business Networking (such as LinkedIn) are prohibited.

3.2.2. All internet access shall be monitored by SMD to determine violation of the BIR's security policies.

3.2.3. Internet access must go through the BIR's firewall. Other ways to access the Internet, such as dial-up or wireless broadband connections to an Internet provider, are prohibited.

3.2.4. Any file downloaded over the Internet shall be scanned for viruses, using approved virus detection software.

4. Physical and Mobile Media Protection

4.1. Confidential and sensitive information contained in portable devices shall be protected using encryption or intricate passwords.

4.2. Users must not leave their PCs unattended without first logging-out or invoking a password-protected screen saver.

4.3. Users shall clear their desk and working areas of sensitive or valuable information after working hours (Clean Desk policy)

5. Asset Classification and Protection

5.1. All information, data and documentation generated or produced by the BIR are considered as proprietary property of and by the BIR.

5.2. A comprehensive up-to-date inventory of assets must be maintained. At a minimum, it must include physical assets, software assets, information assets, services and personnel.

5.3. All BIR information must be classified in terms of its value, legal requirements, sensitivity, and importance to the organization. (Restricted, Confidential, Internal Use, Public)

5.4. All information assets that do not carry any classification marking must be treated as "Confidential."

5.5. Access to Confidential information of unauthorized user must be approved by ACIR and DCIR of the Asset Owner while access to Restricted information must be approved by DCIR and CIR of the Asset Owner.

5.6. Except for Public information, information assets must be encrypted before transmission.

5.7. All documents must be delivered by BIR personnel/messenger only.

6. Enforcement

6.1. Any violation to the BIR's Acceptable Use Policy is considered breach of BIR policies and procedure, and is subjected to disciplinary action in accordance to the BIR's Code of Conduct.

6.2. The management reserves the right to execute or revoke disciplinary actions

7. Reporting

7.1. Users should immediately report to SMD and/or Help Desk should they suspect any actual unauthorized use of their account, or any other violation of security.

ACCEPTABLE USE POLICY ACKNOWLEDGEMENT

BIR users and third parties (partners, contractors, temporary users/s, consultants, third party service providers and taxpayers) who require and have access to the BIR's information or information systems, BIR's equipment, PCs, peripherals, information media and communications infrastructure must indicate their acceptance of the BIR's 'Acceptable Use Policy' and other policies associated with this access through this Acknowledgement Form.

By signing this acknowledgement, the user states that, he/she has understood and agrees to abide by the Acceptable Use Policy and all applicable information security policies. This confirms that the user understands and accepts his/her responsibilities when accessing BIR's information and/or information systems and agrees to comply with future-circulated updates to this policy.

This acknowledgement also confirms to abide to future circulated updates to this policy.

User Acknowledgement:

I, ____, hereby confirm that I have read and understood the Acceptable Use Policy. I acknowledge my responsibilities and agree to abide by all other applicable information security policies set by the BIR.

Signature: ____

Date: ____