REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF INTERNAL REVENUE

REVENUE MEMORANDUM ORDER NO. 67-2010

SUBJECT: Addendum to RMO No. 53-2010 dated June 11, 2010 by prescribing the policies and guidelines on Information and Communication Technology (ICT) Security Infrastructure offenses

TO: All Internal Revenue Officials, Employees and Others Concerned

---

This Order is an addendum to RMO No. 53-2010 dated June 11, 2010 by prescribing the policies and guidelines on Information and Communication Technology (ICT) Security Infrastructure System, defining thereat certain offenses as additional grounds for administrative disciplinary action with their corresponding penalties, which shall form part of **Chapter II, Section 12 (G) entitled "Create and maintain Awareness of the need for information security to be an integral part of the day-to-day operation of business systems",** and **Chapter VII, Section 44 under "Additional Circumstances as Grounds for Administrative Disciplinary Action with their Corresponding Penalties", of the Revised Code of Conduct.**

This Order shall take effect immediately.

(Original Signed)
KIM S. JACINTO-HENARES
Commissioner of Internal Revenue

CHAPTER II – RESPONSIBILITY TO THE BIR

Section 12. Responsibility of Head of Office and other Revenue Employees

G. Create and maintain Awareness of the need for information security to be an integral part of the day-to-day operation of business systems.

Every Revenue Official or Employee shall be responsible in protecting and conserving the Information and Communication Technology (ICT) resources of the bureau. He/She shall be responsible for observing all established policies, procedures and requirements in the ICT environment. He/She shall create and maintain awareness of the need for information security to be an integral part of the day-to-day operation of business systems.

He/She shall also ensure that Security Policies and all pertinent revenue issuances shall not be violated.

Users are responsible for all activities, known or unknown, related to the use of their ID.

Security Breach in the ICT environment shall be classified as follows:

A. Gross Neglect of Duty
- Disclosure of sensitive information without prior management approval
- Unsecured superuser and other powerful accounts
- Disclosure of user id and password without consent
- Failure to disclose to proper authorities any event or incident of violations and/or security breaches discovered by and/or made known to him/her
- Other analogous cases

B. Grave Misconduct
- Unauthorized user access to BIR offices
- Unauthorized access to the operating system
- Unauthorized access to the database
- Unauthorized alterations (addition, modification, deletion) to system objects and files, application, data and logs
- Unauthorized access to the network
- Unauthorized access to application systems
- Unauthorized access to machines (PCs, servers, peripherals, etc.) holding or transmitting applications or data
- Unauthorized access to printed output (reports, correspondences, etc.) and electronic files
- Unauthorized copying of BIR software and data
- Installation of unauthorized software
- Unauthorized access to external storage media (tape cartridges, flash drives, optical media, floppy disks, etc.)

- Unauthorized users gaining access to the system via logged-in workstations
- Adding an unauthorized PC or other devices to the network
- Disclosure of user id and password even with his/her consent
- Misrepresentation or falsification of his/her identity on the internet or in any BIR system or communications
- Disruption of the operations of the BIR's information and communication technology systems
- Unauthorized disabling of hardware, software, monitoring tool installed on any system or network
- Abuse of access privileges
- Unauthorized download, installation, storage or transmittal of software not licensed to the BIR
- Unauthorized probing or cracking of security mechanisms either at BIR or external sites
- Unauthorized establishment of internet or other external network connections
- Unauthorized setting-up of proxy servers
- Other analogous cases

C. Falsification of official document
- Unauthorized alterations (addition, modification, deletion) to printouts (reports, correspondences, etc.) and electronic files
- Other analogous cases

Non-compliance therewith shall constitute as a Grave Offense.

Chapter VII – REMOVAL FOR CAUSE, CLASSIFICATION OF OFFENSES AS PRECRIBED UNDER EXISTING CIVIL SERVICE COMMISSION RULES, AND ADDITIONAL GROUNDS FOR ADMINISTRATIVE DISCIPLINARY ACTION WITH THEIR CORRESPONDING PENALTIES

Section 44. Additional Circumstances as Grounds for Administrative Disciplinary Action with their Corresponding Penalties

Grave Offenses	***Infractions***	***Penalties***
Grave Misconduct as defined in Section 12 (G)	• Disclosure of sensitive information without prior management approval • Unsecured superuser and other powerful accounts • Disclosure of user id and password without consent • Failure to disclose to proper authorities any event or incident of violations and/or security breaches discovered by and/or made known to him/her • Other analogous cases	• 1st Offense, Dismissal
Gross Neglect of Duty as defined in Section 12 (G)	• Unauthorized user access to BIR offices • Unauthorized access to the operating system • Unauthorized access to the database • Unauthorized alterations (addition, modification, deletion) to system objects and files, application,	• 1st Offense, Dismissal

Grave Offenses	***Infractions***	***Penalties***
	data and logs • Unauthorized access to the network • Unauthorized access to application systems • Unauthorized access to machines (PCs, servers, peripherals, etc.) holding or transmitting applications or data • Unauthorized access to printed output (reports, correspondences, etc.) and electronic files • Unauthorized copying of BIR software and data • Installation of unauthorized software • Unauthorized access to external storage media (tape cartridges, flash drives, optical media, floppy disks, etc.) • Unauthorized users gaining access to the system via logged-in workstations • Adding an unauthorized PC or other devices to the network • Disclosure of user id and password even with his/her consent • Misrepresentation or falsification of his/her identity on the internet or in any BIR system or communications • Disruption of the operations of the BIR's information and communication technology systems • Unauthorized disabling of hardware, software, monitoring tool installed on any system or network • Abuse of access privileges • Unauthorized download, installation, storage or transmittal of software not licensed to the BIR • Unauthorized probing or cracking of security mechanisms either at BIR or external sites • Unauthorized establishment of internet or other external network connections • Unauthorized setting-up of proxy servers • Other analogous cases	
Falsification of Official Document as defined in Section 12 (G)	• Unauthorized alterations (addition, modification, deletion) to printouts (reports, correspondences, etc.) and electronic files • Other analogous cases	• 1st Offense, Dismissal