REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF INTERNAL REVENUE

March 05, 2014

REVENUE MEMORANDUM ORDER NO. 15-2014

SUBJECT : Revised Information and Communications Technology (ICT) Security Policy

TO : All Internal Revenue Officials, Employees and Others Concerned

---

I. Objectives

This Order is being issued to:

- Amend Revenue Memorandum Order No. 50-2004 dated November 9, 2004, relative to the policies and procedures on the BIR's Information and Communications Technology Security Infrastructure.
- Define the principles, roles and responsibilities to which all BIR employees and third parties must adhere to when handling information owned by, entrusted to and/or shared with the BIR
- Communicate the accepted requirements to maintain the confidentiality, integrity and availability of information assets
- Maintain awareness of the need of information security and the need to be an integral part of the day-to-day operations of BIR.

II. Scope

The ICT Security Policy document (Annex "A") applies to all BIR employees and third parties (partners, government agencies, contractors, temporary employees, consultants, third party service providers, taxpayers, and the public) who develop, administer, maintain or process (directly or indirectly) BIR information assets.

III. ICT Security Policy

3.1 The ICT Security Policy document defines the high level statement of the overall intention or direction as formally expressed by management. Thus, compliance is mandatory.

3.2 The ICT Security Policy shall have corresponding baseline security standards, guidelines and procedures to ensure proper implementation and control:

3.2.1 Standards – These documents interpret the Information Security Policy Statements for specific technologies. These are technology-directed norms of Information Security for specific systems and security domains.

3.2.2 Guidelines – These documents clarify what should be done and how to achieve the objectives set out in the policies. These are technology-neutral statements of Information Security Policies for specific security domains and/or architectural elements.

3.2.3 Procedures – These documents contain the work steps for the implementation of controls as required by the Information and Communication Technology Security Policy.

3.3 All information asset owners, custodians, users shall have access to the ICT Security documents except for those classified as Confidential to ISG. For third parties, they shall have access to the ICT Security documents that are classified as Public. Updates on the documents shall likewise be communicated upon approval of Information Security Steering Committee (ISSC).

3.3.1 Public – These are information assets that have been explicitly authorized by the owner for public access, through the Internal Communications Division. This classification of information is directly and principally relating to the dissemination of information to the public and its various stakeholders.

3.3.2 Internal Use – These are information assets that are generally used in the conduct of the BIR's operations and do not need special security controls which may remain unlabelled and left unclassified. An explicit authorization should be obtained from the information asset owner (process owner) before releasing INTERNAL USE information to the public, effectively re-classifying the asset into PUBLIC.

3.3.3 Confidential – These are information assets, which compromise or unauthorized disclosure could cause moderate to limited damage to the BIR, should be classified as CONFIDENTIAL. This classification may be used in relation to the Group, Division or Section within the BIR that owns and requires the protection of the information asset.

3.4 The ICT Security documents are classified as follows:

Documents	Information Asset Classification
Information Security Policy	
BIR Information and Communications Security Policy	Public
Acceptable Use Policy	Internal Use
Information Security Risk Management	
Information Security Risk Management	Confidential to ISG
Information Security Standards	
Firewall Baseline Security Standard	Confidential to ISG
Router Baseline Security Standard	Confidential to ISG
Linux Baseline Security Standard	Confidential to ISG
IBM AIX-Unix Baseline Security Standard	Confidential to ISG
Sun Solaris-Unix Baseline Security Standard	Confidential to ISG
Oracle Baseline Security Standard	Confidential to ISG
MS SQL Server Baseline Security Standard	Confidential to ISG
DB2 Baseline Security Standard	Confidential to ISG
Windows 2000/2003 Baseline Security Standard	Confidential to ISG
Windows 2008 Baseline Security Standard	Confidential to ISG
Personal Computer Baseline Security Standard	Confidential to ISG
Wireless LAN Baseline Security Standard	Confidential to ISG
Apache Web Server Baseline Security Standard	Confidential to ISG

Information Security Guidelines	
Password and Login Control Guidelines	Internal Use
Outsourcing and Third Party Access Guidelines	Internal Use
Network Security Guidelines	Confidential to ISG
Internet Security Guidelines	Internal Use
Email Security Guidelines	Internal Use
Telecommuting and Mobile Computing Guidelines	Internal Use
Information Processing Facilities Security Guidelines	Confidential to ISG
Information Asset Classification Guidelines	Internal Use
Application System Security Guidelines	Confidential to ISG
Secure Application Development Guidelines	Confidential to ISG
Information Security Management Procedures	
Information Security Incident Management Procedures	Internal Use
User Account Management Procedures	Internal Use
Information Security Management (Patch and Antivirus) Process	Confidential to ISG
Configuration Change Management Procedures	Confidential to ISG

3.5 Request for a copy or to view the ICT Security documents classified as Confidential to ISG shall require the approval of the Deputy Commissioner – Information Systems Group (DCIR-ISG).

3.6 Information Security Standards, Guidelines and Procedures classified as Internal Use shall have corresponding Revenue Memorandum Orders. For those classified as Confidential to ISG, an Information Systems Group (ISG) Memorandum Orders shall be prepared by Security Management Division (SMD) / IT Planning and Standards Division (ITPSD) and approved by DCIR-ISG.

3.7 The Heads of Offices are responsible and required to monitor the implementation and adherence to the set policies, standards, guidelines and procedures as provided in the BIR ICT Security Policy.

3.8 SMD is the designated custodian of the BIR ICT Security Policy and its Manual. Moreover, SMD together with ITPSD are responsible for the management, maintenance, and accuracy of this document.

3.9 SMD shall review the Manual on an annual basis and/or whenever there are significant events affecting the Bureau such as, but not limited to:

3.9.1 Significant security incidences
3.9.2 New vulnerabilities
3.9.3 Changes to the organizational or technical structure
3.9.4 New government requirements
3.9.5 Legal and contractual obligations

IV. Non-compliance

Non-compliance or violation to set policies, standards, guidelines and procedures as contained in the ICT Security Policy shall subject the offender to immediate disciplinary and/or legal actions.

V. Repealing Clause

This Order supersedes RMO 50-2004 and other related issuances, memoranda, guidelines and/or portion thereof inconsistent herewith.

VI. Effectivity

This Order shall take effect immediately.

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