Annex A

BUREAU OF INTERNAL REVENUE

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECURITY POLICY

Revision History

Version	Date	Author(s)	Revision Notes
1.0	November 20, 2012	Security Management Division (SMD)	

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

The goal of the Information and Communications Technology Security Policy (or the "Policy") is to ensure that the confidentiality, integrity and availability of all pieces of information owned by, entrusted to and/or shared with the Bureau of Internal Revenue (BIR) are protected in a manner that is consistent with:

- The value attributed to it by the BIR
- The risk the BIR will be willing to accept.

1.2 Purpose, Scope, Applicability, and Exception

1.2.1 Purpose

The purpose of the Policy is to define the principles to which all BIR employees and third parties (partners, government agencies, contractors, temporary employees, consultants, third-party service providers, taxpayers and the public) must adhere to when handling information owned by, entrusted to and/or shared with the BIR in any manner or form. It shall cover the following areas:

- Defining the confidentiality, integrity and availability requirements for information used to support BIR's objectives
- Ensuring that accepted requirements are effectively communicated to parties mentioned above who come in contact with such information
- Using, managing and disseminating such information – in any form, electronic or physical - in a manner consistent with the duly accepted requirements.

1.2.2 Scope

This Policy applies to all parties mentioned above who develop, administer, maintain or perform a function on BIR's information systems, and to all information system resource storing, processing, supporting or other similar activities on information owned by the BIR.

1.2.3 Applicability

This Policy shall apply to all information assets of BIR which shall be strictly adhered to by all BIR employees and third parties accessing, processing, transmitting or storing BIR information assets.

1.2.4 Exception

When an information asset owner, custodian, user or a third party cannot comply with any provision of this Policy, a formal request for an exception must be approved and documented. An exception request requires the following:

- Description of the nature of the exception request
- Description of compensating controls
- Remaining operational risks/potential operational impact, if any
- Description of the duration of the exception
- Description of the operational impact if an exception is not granted

Exceptions shall comply with procedures detailed in Section 15 of this document.

1.3 Maintenance of the Manual for the ICT Security Policy

The Security Management Division (SMD) is the designated custodian of the Information Security Policy. It shall therefore, be responsible for the maintenance and review of the Manual for the Information and Communications Technology (ICT) Security Policy (or the "Manual").

The BIR shall review the Policy and its Manual annually and/or whenever there are significant events affecting the BIR such as, but not limited to:

- Significant security incidences
- New vulnerabilities
- Changes to the organizational or technical structure
- New government requirements
- Legal and contractual obligations.

2 INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECURITY POLICY STATEMENT

2.1 Information and information systems, including information about its employees and taxpayers are among the most valuable assets of the BIR. These must be protected against unauthorized disclosure or modification, misuse, destruction or unavailability. Security for these information assets is essential to the BIR operations and overall risk management. Moreover, information security is vital in establishing and sustaining trust between the BIR and its stakeholders, maintaining compliance with relevant regulations, and protecting the BIR's reputation. Information security aims to achieve the following objectives:

- Confidentiality: information must be protected from disclosure to unauthorized individuals, entities or processes.
- Integrity: Information must be protected from unauthorized modification or destruction so that the accuracy, completeness and reliability of the information are assured.
- Availability: Information must be available when and where needed to enable BIR to function efficiently and to ensure that BIR can serve the taxpayers effectively.

2.2 Information security is the process by which the BIR protects and secures the systems, media, and facilities which process and maintain information critical to its operations. It requires data classification and risk management techniques using a balanced and cost-effective combination of security controls covering people, processes and technologies.

2.3 In protecting its information assets, the BIR shall adhere to all applicable laws and regulations. The BIR shall require its employees to meet the highest ethical standards in dealing with taxpayers, third parties and other government agencies.

2.4 The responsibility of protecting and safeguarding information assets rests with all BIR employees. It shall be shared with third parties, who are under the same obligation to protect and safeguard the BIR's information assets.

2.5 Any violation of BIR's information security policies shall result in disciplinary action and/or enforcement of contractual rights and obligations, remedies and/or cause of action by the BIR.

3 ICT SECURITY POLICIES: OVERVIEW

Information security policies enhance the BIR's capability to protect its information assets from loss, damage, unauthorized disclosure or disruption of operations. They shall include the physical and logical protection of systems, processes and stored data that are processed or transmitted within BIR.

The following information security policies provide a set of controls that are based on industry leading practices:

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Acquisition, Development and Maintenance
- Incident Management
- Business Continuity Management
- Compliance

4 ICT SECURITY POLICY

4.1 The ICT Security Policy shall provide requirements for administrative, technical and/or physical security. This is supported by a hierarchy of documents including Information Security Policy standards, guidelines and procedures. To the extent possible, all policies shall be based on current industry best practices.

4.2 This manual shall be approved, published and communicated to all BIR employees and relevant third parties.

This ICT Security Policy shall be reviewed annually, and/or if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.

5 ORGANIZATION OF INFORMATION SECURITY

5.1 Information Security Roles and Responsibilities

5.1.1 The Commissioner of Internal Revenue, through the Information Security Steering Committee (ISSC), shall be responsible for driving the overall information security direction of the BIR.

5.1.2 The Security Management Division (SMD) shall have the overall responsibility for the support and/or monitoring of the development and implementation of information security and related control processes.

Responsibilities of SMD shall include:

- Information Security Policy Development
- Information Security Risk Management
- Security Monitoring and Reporting
- Business Continuity Support
- Support Security Deployment
- Such other related tasks that may be assigned.

5.1.3 The asset owner is responsible for an information asset and is accountable for:

- The determination of information sensitivity and creation of asset inventory,
- Ensuring that appropriate degree of protection is provided,
- The sponsorship of regular audits for protection of information assets, and
- Granting access to information assets.

5.1.4 The information asset custodian shall be responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making back-ups so that critical information will not be lost. They must implement, operate and maintain the security measures determined by the process owners.

5.1.5 The information asset user shall be responsible for the appropriate use of specific information assets, ensuring the security of the information and adhering to all information security policies, standards, guidelines and procedures.

5.1.6 The Internal/Third Party Audit shall assess the design and compliance with information security policies, standards, guidelines and procedures.

5.2 Internal Organization

5.2.1 The BIR Management shall ensure that information security shall be given a high priority in all current and future operational activities and initiatives.

5.2.2 The Information Security Technical Working Group (ISTWG) shall coordinate with the SMD in implementing and maintaining the desired level of information security within the BIR.

5.2.3 The roles and responsibilities shall be clearly defined to protect BIR information assets and to carry out specific security processes.

5.2.4 SMD shall maintain appropriate contacts with relevant authorities (e.g., fire department, police department, National Bureau of Investigation).

5.2.5 SMD shall maintain contact with groups specializing in information security (e.g., Internet forums, security organizations) to ensure that the information security environment is current and complete.

5.2.6 BIR's approach in managing and implementing information security shall be independently reviewed at planned intervals, or whenever there are significant changes to the security implementation, to ensure that it is current and being carried out effectively.

5.3 Addressing Security with Third Parties

5.3.1 BIR shall identify risks to its information and information processing facilities involving third parties and the same shall be communicated to said third parties. BIR shall provide appropriate controls before granting access to third parties.

5.3.2 Access by third parties to the information or information processing facilities shall not be provided until the control mechanisms have been implemented and a contract/Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) has been signed, defining the terms and conditions for the connection or access, thereof.

5.3.3 All third parties who are service suppliers to BIR must formally agree in writing in a public document to follow BIR's information security policies. Any organization, individual and/or other judicial entity with outsourcing contracts with BIR must comply with BIR's Information Security Policy and also provide a service level agreement which shall provide for the performance expected and the remedies available in case of non-compliance.

5.3.4 In any case, contacts with relevant authorities and third parties must be maintained, especially when information security is involved.

6 ASSET MANAGEMENT

6.1 Accountability for assets

6.1.1 The BIR shall have proprietary rights over all information, data, and documentation that it has generated or produced.

6.1.2 External transmission or transfer of information, data and documentation to un-related third parties must require prior authorization.

6.1.3 The responsibility for each item of information, process, data and documents shall be allocated to a specifically designated asset owner or custodian.

6.1.4 The authorization process for new and/or upgrade of information processing facilities is set out below:

6.1.4.1 An authorization process must be implemented for new and/or upgrade of information processing facilities which will be made available to BIR users.

6.1.4.2 New and/or upgrade of facilities must have appropriate management authorization through SMD to ensure that the Policy and other relevant security policies and requirements are met.

6.1.4.3 The use of personal or privately-owned information processing facilities, e.g., laptops, home-computers or hand-held devices, for processing information must have appropriate management authorization through SMD to ensure that the Policy and other relevant security policies and requirements are met.

6.1.5 Rules and guidelines for acceptable use of the BIR's information assets associated with information processing facilities (e.g., use of electronic mail and internet, and mobile devices, especially outside the premises) shall be identified, documented and implemented.

6.2 Asset Inventory

6.2.1 The BIR shall maintain a comprehensive and up-to-date inventory of information assets.

6.2.2 As a minimum requirement, the inventory shall include the following:

6.2.2.1 Physical assets: computer equipment (i.e., personal computers, servers), communications equipment, computer media,

6.2.2.2 Software assets: operating systems, application software purchased and/or developed for BIR use, system software, development tools and utilities,

6.2.2.3 Information assets (information): any data, information or material generated, gathered, compiled, stored or utilized by BIR in the course of its operations, regardless of format or form (either electronic or physical documents),

6.2.2.4 Services: computing and communications services, general utilities (i.e., heating, lighting, power, and air-conditioning),

6.2.2.5 Personnel: BIR's manpower with their qualifications, skills and experience, and

6.2.2.6 Such other relevant and allied inventory.

6.3 Asset Classification

6.3.1 All BIR information must be classified in terms of its value, legal requirements, sensitivity, and importance to the organization.

6.3.2 The classification of each of the information asset shall be reviewed annually.

6.3.3 All BIR information, data and documents shall be processed and stored strictly in accordance with the classification standards.

6.3.4 BIR information, owned and/or entrusted to the Bureau, shall have to be protected in a manner corresponding to its sensitivity and importance. Security measures shall be employed regardless of the media in which information is stored (paper, electronics and so on), the systems which process it (personal computers, firewalls, voice mail systems and so on), or the methods by which it is moved (e-mail, face-to-face conversation and so on).

6.3.5 Information assets with varying classification being transported together, must observe the strictest protection required for the most critical asset.

6.3.6 All BIR information, data, and documents must be stored appropriately according to its level of criticality.

6.3.7 All information assets that do not carry any classification marking must be treated as "Internal Use Information."

6.4 Asset Protection

6.4.1 Requirements for confidentiality or non-disclosure agreements reflecting BIR's need for the protection of information shall be identified and regularly reviewed. The following conditions must be observed:

6.4.1.1 Confidentiality or non-disclosure agreements must be used whenever the BIR's information assets and/or ICT security is involved.

6.4.1.2 All BIR information employees, including third parties, must accept non-disclosure obligations. Users must not disclose BIR information, derived as a result of their access to BIR information assets, to unauthorized parties or any party without prior authorization.

6.4.1.3 Confidentiality or non-disclosure agreements shall be reviewed regularly.

6.4.1.4 All users must re-affirm their non-disclosure obligations annually by signing non-disclosure agreements.

7 HUMAN RESOURCE SECURITY

7.1 Prior to employment

7.1.1 Security roles and responsibilities of employees and third parties shall be defined and documented (i.e., terms and conditions of employment, employee's handbook) in accordance with this Policy.

7.1.2 Background verification checks on all candidates for employment, contractors and third party users must be carried out in accordance with relevant laws, policies, regulations and ethical standards and practices.

7.1.3 The terms and conditions of employment shall include requirements for compliance with this Policy.

7.2 During employment

7.2.1 The BIR must ensure that all employees and third parties accept their information security roles and responsibilities, especially before they are granted access to the BIR's information assets.

7.2.2 All BIR employees must be provided with information security awareness tools (training and reference materials) to enhance awareness and educate them regarding the range of threats, and for them to protect BIR's information assets.

7.2.3 An appropriate summary of the information security policies shall be formally delivered to and accepted by all employees and third parties prior to their commencement of actual work. Security responsibilities shall be included in the evaluation of employee's

and third party's performance. Non-compliance with information security policies, standards, or procedures must be a ground for disciplinary action, up to and including termination, in a formal disciplinary process.

7.3 User's Security Awareness Training

7.3.1 The SMD, in coordination with the Human Resource Development Service (HRDS), shall update the comprehensive information security awareness program.

7.3.2 Each employee must be oriented to information security practices and policies of the BIR. Employees that have technical security responsibilities shall be required to acquire skills that correspond to their individual job roles.

7.3.3 The information security awareness program must be periodically reviewed and evaluated for relevance and effectiveness.

7.4 Termination or Transfer of Assignment

7.4.1 Responsibilities of employees, who are transferred to another assignment or terminated from the service, shall be clearly defined and assigned.

7.4.2 All employees and third-party service providers shall return all of BIR's assets in their possession and proper clearance shall be obtained before being transferred to another assignment or terminated from the service.

7.4.3 All access rights of all employees and third parties to information and information-processing facilities shall be terminated/cancelled and/or adjusted or redefined upon change or removed upon termination of their employment, contract or agreement.

7.4.4 After his/her employment has ended, due to retirement, termination or resignation, or other causes as provided for by laws, the terms and conditions shall continue to be observed for a period of 5 years.

7.4.5 These responsibilities shall be maintained at all times, even beyond the BIR's premises and normal working hours.

8 PHYSICAL AND ENVIRONMENTAL SECURITY

8.1 Secured Areas

8.1.1 Security perimeters shall be used to protect areas that contain information and information-processing facilities.

8.1.2 Secured areas shall be protected from any unauthorized access using appropriate entry controls.

8.1.3 Physical security shall be applied for offices, rooms, facilities and other relevant areas handling information and information-processing facilities.

8.1.4 All critical or sensitive BIR information handling activities must take place in areas that are physically secured and protected against unauthorized use, access, interference and damage.

8.1.5 Buildings and structures that house BIR computers or communication systems shall be protected by adapting physical security measures that shall prevent unauthorized persons from entering and/or gaining access thereto.

8.1.6 Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and/or other forms of natural or man-made disasters shall be designed, applied and practiced.

8.1.7 Physical protection and guidelines for working in secure areas shall be designed, applied and/or practiced.

8.1.8 Activities inside the secured areas shall be documented, monitored and/or reviewed regularly, as the need arises.

8.1.9 A secured area shall have a separate receiving area that shall be used for deliveries. All delivery personnel must not be able to directly access rooms and areas containing information and information-processing facilities.

8.2 Equipment Security

8.2.1 When placing information processing equipment, suitable precautions must be taken to guard against environmental threats or exposures. The equipment shall be operated within the manufacturers' standards.

8.2.2 Computer and communication equipment shall be protected from power failures and other associated electrical disturbance.

8.2.3 There must be no signs indicating the location of BIR's highly secured area to reduce the risk of sabotage or information leakage.

8.2.4 Eating, drinking and smoking inside the secured area are strictly prohibited.

8.2.5 Power, telecommunication and network cabling carrying data or supporting information services must be protected from any unauthorized interception, damage or like violation.

8.2.6 Equipment shall be maintained properly.

8.2.7 Equipment and related peripherals brought in and out of BIR's premises shall be inspected, and/or when required, registered, logged and accompanied by a duly authorized issued gate pass.

8.2.8 Equipment brought out of the BIR premises must be secured at all times.

8.2.9 All equipment containing storage media must be checked by responsible office(s) to ensure that any critical information asset and licensed software are removed, securely overwritten or destroyed prior to disposal, reuse or being declared unserviceable.

8.2.10 Equipment owned by the BIR may only be taken off-site by authorized personnel who have ensured that the relevant security risks have been addressed.

9 COMMUNICATIONS AND OPERATIONS MANAGEMENT

9.1 Operating Procedures and Responsibilities

9.1.1 Operating procedures must be formally authorized, documented and available for official use only.

9.1.2 All changes to BIR's information systems shall follow duly approved change management procedures. The responsible office shall ensure security consideration on new deployments and configuration changes

9.1.3 Duties shall be properly segregated.

9.1.4 All development, test and production facilities, and environments shall be physically and/or logically separated.

9.2 Third Party Service Management

9.2.1 Service delivery from a third party must undergo pre-acceptance checking to ensure that the security controls, service definitions and delivery levels are included in the service level agreement.

9.2.2 All services, reports and records provided by a third party shall be monitored, reviewed and audited regularly and as the need arises.

9.2.3 Whenever there are changes on the terms and conditions of the service agreement, the BIR shall consider the criticality of the operational systems and processes involved, and re-assessment of risks.

9.3 System Planning and Acceptance

9.3.1 The use and utilization of system resources shall be monitored, tuned and projections made for future capacity requirements to ensure required systems performance.

9.3.2 Systems acquisition and implementation procedures shall include clearly defined and approved system acceptance criteria.

9.3.3 Acceptance criteria for new information systems, upgrades and new versions shall be established, and suitable tests of the system shall be carried out prior to acceptance.

9.3.4 All critical systems shall be tested for capacity, peak loading and stress. These systems shall demonstrate a level of performance and resilience that meets or exceeds the technical and operational needs and requirements of BIR.

9.4 Protection against Viruses, Worms and other forms of Malicious and Mobile Code

9.4.1 Detection, prevention and recovery controls mechanism, user awareness program and prohibition to use unauthorized software shall be designed and implemented.

9.4.2 Authorized mobile code shall be operated according to clearly defined security policy.

9.5 Backup and restoration

9.5.1 All BIR servers and key workstations shall be regularly backed-up. These shall be securely retained so that information can be restored with minimum loss in the event of a disaster or corrupted information.

9.5.2 Information System Owners must ensure that the adequate back-up and system recovery procedures are in place.

9.5.3 Back-ups shall be stored in a strategic location, at a sufficient distance to protect from any damage /disaster at the main site or depending on its criticality

9.5.4 Back-ups shall be periodically tested for effectiveness.

9.6 Network Security Management

9.6.1 The network shall be adequately managed and/or controlled to prevent threats and to maintain security for systems and applications using the network, including the transmission of information.

9.6.2 Special controls shall be established to safeguard the confidentiality and integrity of data accessible through external networks, and to protect the connected systems and applications. Special controls may also be required to maintain the availability of the network services and computer connections.

9.6.3 Security features, service levels and related management requirements of all network services shall be included in any network services agreement, whether in-house or outsourced.

9.7 Media Handling

9.7.1 Removable computer media shall be regulated and physically protected in order to prevent data leakage, interruptions and damage to critical information assets.

9.7.2 Using formal procedures, all media shall be disposed securely and safely when no longer required in order to eliminate the risk of information leakage to outside resources.

9.7.3 Procedures shall be established to handle, store and protect the BIR's information assets.

9.7.4 System documentation that is used by administrators and programmers shall be developed, maintained and protected against unauthorized access and use. Access and use to and of these documentations must be restricted to personnel performing official duties only.

9.8 Exchanges of Information and Software

9.8.1 Information and software exchange agreements

9.8.1.1 Formal exchange process shall be established for the exchange of information assets or software within and/or outside the BIR.

9.8.1.2 Agreements shall include security controls to protect the exchange of information through all types of communication facilities between the BIR and external parties, taking into consideration the information asset classification.

9.8.1.3 The risks involved in the use of wireless communications shall be taken into account.

9.8.2 Security of media in transit

9.8.2.1 Physical media shall be properly protected and controlled to prevent the unauthorized disclosure or dissemination of critical information assets while in transit.

9.8.3 Electronic office systems and other forms of information exchange

9.8.3.1 Information obtained from Internet sources shall be verified prior to its operational use.

9.8.3.2 Electronic office systems and other forms of information exchange (e.g., e-mail, BIR official messaging system and so on) shall be monitored and used for official activities only. Users shall not use these facilities for unlawful activities, commercial purposes or personal benefit.

9.8.3.3 Procedures shall be developed to protect information and identify security and operational implications of interconnecting business information systems.

9.8.3.4 Information associated with electronic commerce shall be protected from fraudulent activity, contract dispute, and/or unauthorized disclosure and modification.

9.8.3.5 Controls shall be available to protect information involved in online transactions.

9.8.3.6 Integrity of information in publicly available systems shall be protected from unauthorized modification.

9.8.3.7 PBX systems or other systems that may be used for voice communications shall be defined and supported in accordance with the same security principles as those used for data communications.

9.9 Logging and Monitoring

9.9.1 Audit logs of user activities, exceptions and information security events shall be maintained and monitored regularly.

9.9.2 Logging facilities and log information shall be protected against tampering and unauthorized access.

9.9.3 Administrator and system operator activities shall be logged and reviewed regularly.

9.9.4 Fault logs shall be maintained analyzed periodically and/or as the need arises for its impact and appropriate action.

9.9.5 Mechanisms for time synchronization for accurate logging of events on the network shall be employed and managed.

10 ACCESS CONTROL POLICY

10.1 Access Control Policy

10.1.1 All access to information, information processing facilities and operational processes shall be controlled to ensure that the BIR and its employees have available electronic resources for them to work effectively and efficiently. This process shall be established, documented and reviewed.

10.1.2 Access to servers, operating systems, databases and applications shall only be granted for official purpose and limited based on their role.

10.2 User Access Management

10.2.1 User registration and revocation process shall be strictly observed.

10.2.1.1 User-IDs shall uniquely identify a single user. Re-use or multiple-use of user-IDs is prohibited.

10.2.1.2 A user-ID and a strong password are required for access to the information systems and services.

10.2.1.3 A formal registration process shall be in place for granting access to all information systems and services.

10.2.1.4 A formal revocation process shall be in place for revoking access to all information systems and services.

10.2.2 System privileges of all users, systems and standalone programs shall be restricted on a need-to-know basis. Privileges shall be extended only when there is a legitimate and official need for such privilege, which shall be approved accordingly.

10.2.3 Allocation of passwords to users shall be controlled through a formal process.

10.2.4 User accounts, access rights and privileges shall be periodically reviewed and validated. Any inactive accounts shall be disabled and removed using a formal process to maintain effective control over access to information and other services.

10.3 User Responsibilities

10.3.1 All users must adhere to the information security policies, standards, guidelines and procedures of BIR and shall indicate their agreement through the BIR's Acceptable Use Policy. (See Attachment A for the Acceptable Use Policy)

10.3.2 Users must not leave a workstation, that has an active logon session, unattended and unprotected.

10.3.3 A clear desk policy for papers and removable storage media, and a clear screen policy for information processing facilities shall be followed by all employees.

10.4 Network Access Control

10.4.1 Access to networks and network services (i.e., internet, e-mail) shall be controlled on the basis of official purpose and security requirements, and access control rules defined for each network. Access to network devices shall be limited to duly authorized personnel only.

10.4.2 External connections shall be protected by enforcing prescribed authentication and/or encryption methods, the strength of which must comply with relevant laws and regulations. Remote user access shall be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

10.4.3 Automatic equipment identification (e.g., through MAC or IP addresses) shall be considered as means to authenticate connections from specific locations and equipment.

10.4.4 Procedures shall be developed to protect access to the system through remote configuration ports and other forms of access. Ports, services and similar facilities installed on computers or network facilities, which are not specifically required for any official purpose, shall be disabled or removed.

10.4.5 Separation of logical network domains shall be adopted to manage groups of information services, users, and information systems on the network.

10.4.6 The capability of users to connect to shared networks shall be restricted and in line with the access control policy and requirements of the business applications.

10.4.7 Networks shall implement routing controls to ensure that computer connections and information flows do not breach the access control policy of the applications. The BIR's information and communication systems shall restrict access to computers that can reach over the BIR's networks. These restrictions may be implemented via routers, gateways, front-end telecommunications processors, and other network devices.

10.5 Wireless Access Control

10.5.1 Additional authentication controls shall be implemented to control access to wireless networks. In particular, special care is needed in the selection of controls for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.

10.5.2 A password management system shall be in place to manage and ensure acceptable passwords.

10.6 Operating System Access Control

10.6.1 Secure log-on procedures shall be observed.

10.6.1.1 Access to operating system services shall be via a secure log-on procedure only.

10.6.1.2 The log-on procedure shall not disclose information about the system in order to avoid providing an unauthorized user with information that could access the system.

10.6.2 User identification and authentication shall be implemented.

10.6.2.1 All users must have a unique identifier for their sole use so that activities can subsequently be traced to the responsible individual.

10.6.2.2 User IDs shall not give any indication of the user's privilege level.

10.6.3 A password management system shall be in place to manage and ensure acceptable passwords.

10.6.4 Controls shall be in place on the use of tools and utility programs that might be capable of overriding system and application controls.

10.6.5 User connectivity shall automatically be disconnected from the BIR's network after a certain period of inactivity. The user must then logon again to re-connect to the network.

10.6.6 Restrictions on connection times shall be used to provide additional security for high-risk applications.

10.7 Application and Information Access Control

10.7.1 Users of application systems, including support staff (technical support, application developer), must be provided with access to information and application system on a least-privilege basis and official requirements. Services and applications not for general access shall be restricted by an access control list as defined in the access control policy.

10.7.2 Systems handling sensitive information shall be placed in a secured location or in a dedicated computing environment.

10.8 Mobile Computing

10.8.1 Remote access to BIR information assets from public network using mobile computing facilities must only take place after successful identification and authentication, and with suitable access control mechanisms in place.

10.8.2 All mobile computing facilities shall be used in a secured environment, using cryptographic controls for communication purposes as required by the BIR.

10.9 Telecommuting

10.9.1 The BIR shall only authorize telecommuting activities if they are satisfied that appropriate security arrangements and controls are in place and observed, and that these comply with the BIR's Policy.

10.9.2 Off-site computer usage is only allowed if the user has an approved authorization from the concerned office. Usage is restricted to business; therefore, users must be aware of the accepted terms and conditions of use which includes the adoption of adequate and appropriate information security measures set by BIR.

11 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

11.1 Security Requirements of Information Systems

11.1.1 Statements of business requirements for new information systems, or enhancements, to existing information systems shall specify the requirements for security controls.

11.1.2 Information security requirements shall be identified and agreed on prior to the development and/or implementation of information systems.

11.1.3 Applications developed by BIR shall adhere to an accepted systems development, maintenance methodology and to the security requirements reflecting business needs.

11.1.4 Third party-developed applications shall adhere to the BIR policies and standards. Customizations made to third-party software shall likewise conform to BIR's policies and standards.

11.1.5 Systems security requirements shall be defined based on appropriate system risk assessment.

11.1.6 Correct Processing in Applications

11.1.7 Data input to application systems shall be validated to ensure that it is correct and appropriate.

11.1.8 Validation checks shall be incorporated in applications to detect malformed input either through processing errors or deliberate acts.

11.1.9 Message integrity shall be preserved.

11.1.9.1 Where there is a requirement to ascertain authenticity and protect the integrity of the message content, appropriate controls shall be considered.

11.1.9.2 Assessment of security risks shall be carried out to determine if the message integrity is required, and to identify the most appropriate method of implementation.

11.1.10 Output data from an application shall be validated to ensure that the processing phase of the stored information is correct and appropriate.

11.2 Cryptographic Controls

11.2.1 Encryption shall be used to protect the confidentiality of electronic information.

11.2.2 Cryptographic keys used in encryption shall be maintained confidential and protected. Key management shall be in place to support cryptographic activities.

11.3 Security of System Files

11.3.1 Installation of software on operational systems shall have procedures in place.

11.3.2 Access to system development, test environments and test data shall be logged and monitored periodically.

11.3.3 Access to operational program libraries and source codes shall be restricted unless access is granted when there is an official need.

11.4 Security in Development and Support Processes

11.4.1 Formal change control procedures shall be put in place.

11.4.1.1 Formal change control procedures shall be utilized, for all changes, to systems. All changes to programs shall be properly documented, authorized and tested in a test environment before moving to the production environment.

11.4.1.2 The change control processes shall be used for all changes (including configuration changes) to software, hardware and communication links.

11.4.2 Proper segregation of duties shall be observed for incompatible duties. Developers must not have access to production systems.

11.4.3 Risk to modifications of software packages shall be properly assessed and managed.

11.4.4 Controls shall be in place to prevent information leakage.

11.4.5 Outsourced software development shall be supervised and monitored by the BIR.

11.4.6 A process for patch management, vulnerability assessment and penetration testing activities shall be in place.

11.4.6.1 All application systems shall be properly and thoroughly evaluated against the BIR's policies and standards prior to migration to production.

11.4.6.2 Updates shall be tested in a test environment for compatibility prior to deployment to production.

11.4.6.3 Technical review of applications, after operating systems changes, shall be in place to ensure that there is no adverse impact on operations and security.

11.4.6.4 Information on technical vulnerabilities shall be obtained and managed to reduce the BIR's exposures to such vulnerabilities as appropriate measures are taken to address the associated risks.

12 INFORMATION SECURITY INCIDENT MANAGEMENT

12.1 Reporting Security Related Vulnerabilities, Incidents, Weaknesses and Malfunctions

12.1.1 Formal procedures must be established for the monitoring of information security vulnerabilities, alerts and incidents in BIR's servers and network.

12.1.2 A formal incident reporting procedure must be established and disseminated to all employees and third parties. All BIR employees must be made aware of their responsibility requiring the reporting of any information security events immediately.

12.2 Management of Information Security Incidents and Improvements

12.2.1 A formal mechanism procedure shall be developed and established to quantify and monitor all types, volumes and cost of information security incidents.

12.2.2 Responsibilities and procedures for management of information security incidents shall be strictly followed, reported and documented.

12.2.3 Evidence shall be carefully stored, handled and controlled during its gathering, control and storage. Internal procedures shall be developed, implemented and followed for the collection, maintenance and presentation of evidence.

12.3 Learning from Information Security Incidents

12.3.1 Corrective and preventive action plans shall be prepared to prevent the recurrence of the same or similar incidents.

12.3.2 Incident reports shall be analyzed to identify the trends of the types of incidents occurring. Appropriate preventive action shall be undertaken to address the happening thereof.

12.3.3 A summary of the incident reports shall be prepared and distributed by SMD to the BIR's concerned office who reported the incident after the incident has been addressed and closed.

13 BUSINESS CONTINUITY MANAGEMENT

13.1 BIR shall adopt a process whereby continuity in business management shall be assured, developed and maintained in case of a disaster.

13.2 Information security shall be included in BIR's business continuity management program.

13.3 Events that can interrupt business processes, along with the probability and impact as a result thereof and their consequences to information security shall be identified and recovery procedures shall have to be developed.

13.4 A business continuity management framework shall be established and used for consistency and identification of needed priorities for testing and maintenance.

13.5 Business continuity plans shall be tested, maintained and re-assessed.

13.6 The business continuity plan shall be tested regularly to ensure its effectiveness.

13.7 It shall be updated to reflect any major changes to business practice or technology.

13.8 It shall be able to address all types of situations, from partial to total loss, in the worst case scenario of a location, to ensure that critical business information can be recovered and restored.

14 COMPLIANCE

14.1 Identification of Applicable Legislation

14.1.1 The design, operational management and use of BIR's information systems and related facilities shall comply with all applicable laws, regulations or other contractual security obligations and similar requirements.

14.2 Compliance with Legal Requirements

14.2.1 Procedures must be implemented to ensure compliance with relevant laws and regulations with respect to intellectual property rights vested on the use of proprietary software products.

14.2.2 Users must be aware that all the information assets created, distributed, accessed or managed shall remain as property of the BIR. The BIR reserves the right to monitor and/or audit any activity in relation thereto, to ensure compliance with the information security policy at any given time.

14.2.3 Data protection and privacy of the BIR and third-party information shall be ensured.

14.2.3.1 Data protection and privacy requirement shall be ensured under relevant laws and regulations, including all information obtained by employees.

14.2.3.2 A BIR-wide data protection and privacy policy shall be developed, implemented and communicated to all employees involved in the processing of the BIR and third-party information, for their strict compliance.

14.2.4 Unauthorized use of information processing facilities shall be prohibited and dealt with in accordance with the applicable laws and regulations.

14.2.5 All relevant laws and regulations for cryptographic controls shall be identified, implemented and strictly complied with.

14.3 Compliance with Security Policies and Technical Standards

14.3.1 All heads of offices shall be responsible for ensuring that appropriate information security measures are implemented, observed and strictly followed in their respective areas.

14.3.2 Information systems shall be checked regularly to determine strict compliance with all relevant information security standards.

14.4 Information Systems Audit Consideration

14.4.1 Audits of operational information systems shall be planned, adhered to and reviewed periodically with the knowledge and confirmation of the asset owner to minimize the risk of disruption to business processes.

14.4.2 Access to information system audit tools shall be protected to prevent any possible unauthorized use and misuse.

15 NON-COMPLIANCE

Non-compliance with this policy shall be immediately dealt with in accordance with applicable laws, regulations, and issuances of the BIR and Civil Service rules.

16 WAIVER CRITERIA

16.1 This document form is intended to address information security requirements of the BIR. Requests for Waivers must be formally submitted to the SMD, including justification and benefits attributed to the waiver, and must be approved by the ISSC.

16.2 The waiver shall only be used in exceptional situations and only after performing risk analysis examination to determine and establish its implications of noncompliance.

16.3 The waiver shall be granted for a specified period of time only, subject to a maximum period of one (1) year. A reasonable time prior to the completion thereof, a request for extension may be granted if necessary.

16.4 The terms of the waiver shall be limited to, and not to exceed, the three (3) consecutive terms only.

16.5 The waiver shall be monitored by SMD to ensure compliance with the specified period time and exception.

17 REPEALING CLAUSE

All memoranda, guidelines and/or related issuances inconsistent with this Policy are hereby repealed, revised, amended and/or superseded accordingly. Unaffected portions thereof shall remain in full force and effect.

18 DEFINITION OF TERMS

Access control
A mechanism used to protect the access to an asset (e.g., physical access control is a lock on the door, while logical access control could be a user-ID).

Asset(s)
Anything of value to the BIR.

Asset management
The process of maintaining complete and accurate information about the BIR assets. This includes a formal log or inventory of assets, confirmation as to the ownership and/or user thereof, an audit trail of changes made to the asset, and process of maintaining information thereof.

Baseline
The minimum security level for the use, protection and/or maintenance of the asset.

Best practice
The term used to refer to the most desirable or preferred solutions to be used.

Change management
Process of controlling changes to the infrastructure or to any aspect of services, enabling the approval of changes to achieve minimum disruption thereto. Changes may include configurations, upgrades, replacements or the introduction of new or additional hardware, software, networks and telecom providers and like services.

Compliance
Adherence to the BIR policies, standards and procedures including other regulations and laws.

Data center
A centralized secured location that houses significant information processing assets. Data centers shall typically have physical access controls, raised floors, fire protection equipment, power and air conditioning, and other systems to provide an environment suitable for the housing of data processing, networking and communication equipment.

Encryption
A tool used to protect the confidentiality of electronic information

Guideline(s)
The instructions, directives and other clarificatory statements on what should be done and how in order to achieve objectives set out in the policy.

Incident management
The process of restoring and/or returning to normal service after a disruptive event has occurred (e.g., virus attack, network intrusion). The process must be designed to regain normal operations as quickly as possible and with minimal disruption to the operations.

Information asset custodian
Any personnel, group or office with physical or logical possession of information belonging to the BIR.

Process owner
Any personnel, group or office with approved responsibility involving the management for controlling the production, development, maintenance, use and security of assets.

Information security
The process for which information assets and information processing facilities are protected from breaches of confidentiality, integrity and availability which may include unauthorized access, use, disclosure, modification or destruction and other similar events.

Information security incident
An alert or indication of a possible security breach has occurred or may be taking place.

Information asset user
Any personnel, group or office given the required and explicit authorization to access, modify, delete, and/or utilize information by the process owner.

PCs
All end-user computers, including personal computers, laptops, desktops and notebook computers and like equipment.

Policy
A high-level statement of the overall intention or direction as formally expressed by management. It is technology independent. It states general goals and objectives, without necessarily stating how those goals and objectives will have to be accomplished.

Procedure
Detailed steps that personnel must follow.

Security incident
A deliberate or accidental event that may lead to an actual or potential breach against the following:

- Confidentiality, where information is disclosed to unauthorized persons or someone who is not permitted to have it;
- Integrity, where access to information is altered and/or manipulated without permission;
- Availability, including anything that hinders ongoing operations and job functions

Standard
A norm, rule, or requirement that shall establish uniform technical criteria, methods, processes and practices.

Telecommuting
The use of communications technology that enables BIR personnel, group or office to work outside of the BIR or other alternative sites or other locations.

Third Party
Any person organization, or other juridical entity that is not connected with, or is independent of the BIR, which have operational connections/contractual commitments with the BIR, or service provider, or operator of assets on behalf of the BIR. A Third Party may refer to contractors, temporary employees, consultants, and other service providers.