# Table of Contents

1. Overview

2. Definition of Terms

3. Security Policies
   3.1 General Policies
   3.2 Electronic Mail
   3.3 Network Security
   3.4 Server Security
   3.5 Intranet Security
   3.6 Internet Security
   3.7 Extranet Security
   3.8 Wireless Communication / Mobile Tele-Working
   3.9 Virtual Private Network (VPN)
   3.10 Firewall Security
   3.11 Internet DMZ Equipment
   3.12 Database Security
   3.13 Dial-In Access
   3.14 Remote Access
   3.15 Analog / ISDN Line Security
   3.16 Internal Lab Security
   3.17 DMZ Lab Security
   3.18 Information Sensitivity
   3.19 User Account, Password, and Logon
   3.20 User Account Management
   3.21 Acceptable Use of Computer Equipment
   3.22 Acceptable Encryption Use
   3.23 Acquisition Assessment
   3.24 Audit
   3.25 Risk & Vulnerability Assessment / Penetration Testing
   3.26 Third Party / Outsourcing / Proof-of Concept (POC)
   3.27 Third Party Information Disclosure Security

4. Responsibilities
   4.1 Security Management Division, IPQS
   4.2 Network / System Administrators
   4.3 Database Administrators
   4.4 Division Chiefs / Heads of Offices
   4.5 Users
1. Overview

Information is a vital asset to the Bureau of Internal Revenue (BIR). Information is used in every aspect of BIR’s business, from processing payments to investment decisions. Without the right information, the BIR would be unable to fulfill its responsibilities to Department of Finance, management, staff, and the taxpayers. Increasingly, the BIR is reliant not only on information, but on the controls over the input of information to computer systems, and the operation of the computer systems themselves.

The Security and Access Control Architecture of System for the Bureau of Internal Revenue Information & Communications Technology was designed to:

- Prevent and address unauthorized access to machines, network, applications, data and other technical resources;
- Facilitate monitoring of security related events;
- Ensure that security breaches are detected and rectified;
- Ensure that an acceptable level of service is provided to authorize users who wish to access the Integrated Tax System.

This document provides a description of the security policies and procedures that employees, contractors, Third-Party Vendors, and any other information system user shall follow.

2. Definition of Terms

Access Control Server – a computer that stores users with log-in names and passwords ensuring system's security.

Access Control List (ACL) – Lists kept by routers to control access to or from the router for a number of services (e.g. to prevent packets with a certain IP Address from leaving a particular interface on the router)

Application Service Provider (ASP) – ASP’s combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a BIR-owned and operated application. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things.

Approved Electronic File Transmission Methods – Includes supported FTP clients and Web browsers.

Approved Electronic Mail – Includes all mail systems supported by the SSD-ISOS (IT Support Team). If you have a business need to use other mailers contact the appropriate support organization.

Business Critical Production Server – A server that is critical to the continued business operations of the Bureau.

Challenge Handshake Authentication Protocol (CHAP) - An authentication method that uses a one-way hashing function. Data link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVS endpoint within a user’s access channel in a frame relay network, and has local significance only to that channel

Circuit – For the purpose of this policy, circuit refers to the method of network access, whether it’s through traditional ISDN, Frame Relay, etc., or via VPN/Encryption technologies.

Company Information System Resources – These include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.
**Credentials** – Something you know (e.g. a password or pass phrase), and/or something that identifies you (e.g. a user name, a fingerprint, voiceprint, retina print), that are presented for authentication.

**Dial-Up Connection** – is a switched circuit connection because a call is automatically switched through its destination. It allows the agency to access the Internet over standard telephone lines via high speed modems. However, subscribers will share a high speed modem from its Internet Service Provider in accessing the internet.

**DMZ (de-Militarized Zone)** – Networking that exists outside of the Bureau’s primary corporate firewalls, but is still under BIR administrative control.

**Encryption** – Secure BIR sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography.

**Envelopes Stamped Confidential** – You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

**Email or Electronic Mail** – an electronic transmitted mail. It allows you to exchange electronic message that is more reliable and faster than postal mail to anyone around the world with an Internet. Email is most widely used Internet service.

**Executable** - a file that contains a program - that is, a particular kind of file that is capable of being executed or run as a program in the computer.

**Expunge** – To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as part of Norton Utilities. Otherwise, the PC or Mac’s normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

**External Connections** – External connections include, but not limited to, third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.

**Extranet** – a private network which uses Internet protocols and extends beyond organization premises. It is accessible by a subset of both internal (inside the company) and external users.

**Firewall** - protects a computer network from unauthorized access. Firewalls may be hardware devices, software programs, or combination of the two. A firewall typically guards an internal network against malicious access from the outside. It may also be configured to limit access of internal users to the outside.

**Front-end telecommunications processor** – a small computer used to handle communications interfacing with another computer.

**Gateway** - a network point that acts as an entrance to another network. It may also be any machine or service that passes information from one network to another network across the Internet.

**Individual Access Controls** – are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the `chmod` command. On Mac’s and PC’s this includes using passwords on screensavers, such as Disklock.

**Information and Communication Technology** – the totality of the means employed to systematically collect, process, store, present and share information. It encompasses computers, telecommunications and office system technologies, as well as accompanying methodologies, processes, rules and conventions.
Internal (lab) – A lab that is within the Bureau’s corporate firewall and connected to BIR corporate production network.

Intranet – a company-wide web accessible only to company/organization’s members, employees, or others with authorization

Internet – a worldwide interconnection of thousands of computer networks and databases.

Internet Hosting - a business of housing, serving and maintaining files for one or more website.

Internet Services – Services running on devices that are reachable from other devices across a network. Major internet services include DNS, FTP, HTTP, etc.

Lab – A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.

Lab Owned Gateway Device – A lab owned gateway device is the lab device that connects the lab network to the rest of the Bureau’s network. All traffic between the lab and the corporate production network shall pass through the lab owned gateway device unless approved by SMD-IPQS.

Lab Network – A “lab network” is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to the Bureau nor affect the production network.

Mailbox – a storage space that stores an individual’s electronic mail messages.

Network Support Organization – Any SMD-IPQS approved support organization that manages the networking of non-lab networks (This is the equivalent of the SSD-ISOS).

Operating System (OS) shell – an interface between the user and the core of the operating system (kernel). It acts as an interpreter or translator. It accepts commands issued by the user, interprets what the user types and executes the program specified.

Penetration Testing – a covert intrusion under a controlled and managed environment.

Ping – a standard network utility which can be used to determine if a remote device (such as Web or any server) can be reached on the network and the speed of the network connection.

Physical Security – Means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. If it is a laptop or other portable computer, never leave it alone. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive materials in a locked drawer or cabinet.

Private Link – A private link is an electronic communications path that the Bureau has control over its entire distance. For example, a computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. BIR has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which the Bureau has established private links include all announced acquisitions and some short-term temporary links.

Production Network – The “production network” is the network used in the daily business of the Bureau. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to the Bureau employees or impact their ability to do work.

Proof-of-Concept (POC) – A system or a solution provided by a third party at no cost to the Bureau which that may be accepted or adopted if proven beneficial to the Bureau.
**Proprietary Encryption** – An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, and individual, or the government.

**Protocol** – a formal set of rules and conventions determining how devices communicate on the network; protocols are like languages; devices must use the same protocol in order to communicate.

**Risk** – Those factors that could affect confidentiality, availability, and integrity of the Bureau’s key information assets and systems.

**Router** – a physical device that joins multiple networks together.

**Server** – a computer or device on a network that manages network resources such as storing files, manages one or more printers, manages network traffic or processes database queries.

**Sensitive Information** – Information is considered sensitive if it can be damaging to the Bureau or its customers’ dollar value, reputation, or market standing.

**Spam** – an unsolicited bulk e-mail on the Internet. It includes chain letters, items for sale, get rich quick scams or any other unwanted e-mail that people often receive.

**Sponsoring Organization** – The BIR organization who requested that the third party has access into BIR.

**Telco** – A Telco is the equivalent of a service provider. Telcos offer network connectivity, e.g. T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as ‘baby bells’; although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI or Basic Rate Interface – a structure commonly used for ISDN service and PRI or Primary Rate Interface – a structure for voice/dial-up service.

**Telnet**¹ – allows users to connect and access another computer on the Internet. It offers users the capability to use computer resources of other organizations.

**Third Party** – an entity that markets an accessory hardware product for a given brand of computer equipment or provides services / solution for ICT solutions. This may also be referred to as the contractor, vendor or application service provider.

**Traffic** – Mass volume of unauthorized and/or unsolicited network spamming/flooding traffic.

**Transmission Control Protocol (TCP)** – one of the main protocols in TCP/IP network. It enables two hosts to establish a connection and exchange streams of data. It guarantees delivery of data and the packets in the same order in which they were sent.

**User Authentication** – A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

**Unauthorized Disclosure** – The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

---

¹ Source NCC Memorandum Circular No. 2000-01: Prescribing Planning & Managing the Agency’s IT Infrastructure for connection to the Government-Wide Network thru RP-Web

**User Datagram Protocol (UDP)** – connectionless protocol that runs on IP networks. UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used for broadcasting messages over the network.

**Vulnerability Assessment** – an automated process of proactively identifying vulnerabilities of computing systems in order to determine if and where a system can be exploited and/or threatened and provide appropriate recommendation to address those weaknesses.

**Web Browser** – a software used to make contact with websites.

3. **Security Policies**

3.1 **General Policies**

3.1.1 The use of email facilities and similar communication facilities of the Bureau shall be strictly for official business purposes only. Such facilities shall not be used for any unlawful, commercial activities or for any personal financial gains.

3.1.2 All messages sent over Bureau’s ICT systems are the property of the Bureau. Bureau’s management reserves the right to check all information stored in or transmitted by these systems. The Bureau’s ICT systems are for official use only where there is no privacy in any information stored in or sent through these systems.

3.1.3 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 and shall be approved accordingly.

3.1.4 Software and other files shall not be loaded on the computers unless a virus check is performed using an authorized/approved virus-scanning program. It is a violation of this policy to disable any virus-checking facilities installed on any system or network.

3.1.5 Any breach of the security policies stated herewith shall be reported to the Security Management Division of Information Planning and Quality Service (SMD-IPQS) using the Security Violation Report Form (Annex A). SMD-IPQS shall initiate an investigation on the nature of said violation and the corresponding penalty to be imposed using the Security Incident Handling Form (Annex B).

3.1.6 Whenever a user's computer or email account is monitored for investigative or disciplinary purposes, the Head of Office of the concerned user shall be promptly informed of the activity.

3.1.7 All investigations of alleged criminal and/or abusive conduct shall be held with strict confidentiality to preserve the reputation of the suspected party until charges are pursued and/or disciplinary actions are taken.

3.2. **Electronic Mail Policies**

3.2.1 The Bureau’s email systems shall be used for official activities only. Users shall not use email facilities for unlawful activities, commercial purposes or personal financial gain.

3.2.2 Passwords shall never be shared or exposed to anyone besides the authorized users and unauthorized use of email accounts other than those assigned to a particular user is strictly prohibited. Passwords that are lost or are suspected to be lost, stolen, or disclosed, shall be reported to the SMD-IPQS immediately.
3.2.3 The contents of email may be monitored to support operational, maintenance, auditing, security and investigative activities. Systems Support Division of Information Systems Operations Service (SSD-ISOS) may review the contents of a user’s mailbox during the course of problem resolution / investigation upon recommendation and in coordination with SMD-IPQS.

3.2.4 BIR cannot guarantee that electronic communications will be private. Users should be aware that electronic communication can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, electronic communications can be accessed by others in accordance with this policy.

3.2.5 Users shall not use vulgar, obscene or insulting remarks in e-mail messages.

3.2.6 Bureau’s sensitive information must not be forwarded outside the Bureau without prior approval of the Deputy Commissioner of Information Systems Group (DCIR-ISG). Sensitive information shall not be forwarded via any means unless it is critical to business and is encrypted in accordance with the Acceptable Encryption Policy.

3.2.7 Mailbox contents, whether user or the central repository, shall be backed-up on a weekly basis (every Saturday) by the Email Administrator. Backup of email messages shall be retained for one (1) week.

3.2.8 Executable file attachments shall be automatically rejected to prevent the spread of virus.

3.2.9 E-mail messages which are no longer needed for business purposes shall be regularly purged by users from their personal email account. This will increase storage space as well as simplify records management considering that regular email accounts are only entitled to 4 MB storage space.

3.2.10 Heads of Offices are required to submit a request for email account revocation using the Email Account Request Form (Annex C) for their personnel who are no longer connected with the Bureau.

3.2.11 Forwarding of chain letters and other spam mails is strictly prohibited to prevent virus proliferation.

3.2.12 Users are prohibited from allowing anyone else to use their electronic mail account unless a specific published business case by BIR warrants otherwise.

3.2.13 Only the SSD-ISOS shall be allowed to add members to a BIR created and approved distribution list.

3.2.14 Users are prohibited from reading or attempting to read any other user’s electronic communications unless a specific published business case by BIR warrants otherwise.

3.2.15 A legal recipient disclaimer will be automatically added to all external electronic mail messages.

3.2.16 Users shall not misrepresent or falsify their identity on the Internet or in any BIR communications. The user name, organization and other company specific information shall be included in the message or posting.

3.2.17 Users shall refrain from opening electronic mail or suspect attachments from which they do not know the sender or when the subject of the message seems inappropriate. Users shall notify their e-mail administrator who will take appropriate action.
3.2.18 Official company records communication through electronic mail shall be identified, managed, protected, and maintained as long as they are needed for ongoing operations, audits, legal actions, or any other known purpose.

3.2.19 If sensitive, confidential, and/or private information is or is suspected to be lost or disclosed to unauthorized parties, the SSD-ISOS shall be notified immediately.

3.2.20 If unauthorized use of BIR information systems has taken place or is suspected, the SSD-ISOS shall be notified immediately.

3.2.21 All unusual systems behavior, such as missing files, frequent system crashed, misrouted messages, and other similar activities occur, the SSD-ISOS shall be notified immediately.

3.2.22 The specifics of any possible security problems shall be kept confidential to immediate management and security personnel.

3.2.23 Users shall not probe security mechanisms at either BIR or other Internet sites, nor use and/or possess tools for cracking information security unless express written permission is obtained by the Security Management Division, IPQS.

3.2.24 Transmission of any material, document, information that is confidential in nature, in violation of any of the existing policies of the Bureau, department of Finance, and the Philippine Government is prohibited.

3.3 Network Security Policies

3.3.1 Information and Communication Technology (ICT) systems shall be used for business purposes only.

3.3.2 Only authorized Network Administrator shall do all network configurations. Likewise, access to all network devices shall be strictly limited to authorized technical personnel only.

3.3.3 Request for changes to network configuration(s) should be done in writing and duly approved by Chief of SSD-ISOS and Computer Operations Networking and Engineering (CONE) Head for National Office (NO) and Revenue Data Centers (RDC), respectively before corresponding Network Administrator acts on such requests.

3.3.4 All changes to computer networks (including, but not limited to loading new communications software, changing network addresses, reconfiguring routers, adding dial-up lines, and the like) shall be documented and communicated to SMD-IPQS. All emergency changes to the network must only be made by and reported to authorize personnel (Network Administrators) immediately.

3.3.5 All internal network devices (routers, firewalls, access control servers, etc.) shall have unique passwords kept in a secure encrypted form, or other access control mechanisms.

3.3.6 Bureau’s information and communication systems shall restrict access to the computers that users can reach over the Bureau’s networks. These restrictions shall be implemented via routers, gateways, front-end telecommunications processors, and other network devices.

3.3.7 Use of network tools native to the operating system like ping, telnet, arp, etc. shall be limited only to authorized personnel.
3.3.8 The Bureau reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.3.9 Connection to the Bureau’s network shall not be given to any external party unless approved by the DCIR-ISG.

3.3.10 Dial-up connections of consultants, existing contractors and prospective bidders to the Bureau’s network shall only be allowed upon the approval of the DCIR-ISG.

3.3.11 The SSD-ISOS in coordination with Network Administrators of all sites, shall maintain a current inventory of the Bureau’s network facilities including telephone, extranets, intranets and internet.

3.3.12 To positively identify the calling party, all dial-up connections to the internal computer data network shall employ extended user authentication.

3.3.13 Firewall(s) must be in place such that access to connected systems shall be restricted to authorized users only.

3.3.14 No local user accounts shall be configured on the router.

3.3.15 Routers, hubs, modems, and other networking hardware should be strategically located so that these may not be easily tampered with by unscrupulous persons.

3.3.16 The following should be disabled:

- Internet Protocol (IP) directed broadcasts
- Incoming packets at the router sourced with invalid addresses (such as RFC1918 address)
- Transmission Control Protocol (TCP) small services
- User Datagram Protocol (UDP) small services
- All source routing
- All web services running on router

3.3.17 Access rules shall be added as business needs arise.

3.3.18 Each router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

3.4. Server Security Policies

3.4.1. Servers shall be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable

3.4.2 The most recent security patches must be installed on the system as soon as possible, the only exception being when immediate application would interfere with business requirements.

3.4.3 Servers should be physically located in an access-controlled environment.
3.4.4 Servers shall be specifically prohibited from operating from uncontrolled cubicle areas.

3.4.5 Always use standard security principles of least required access to perform a function.

3.4.6 Do not use powerful accounts (such as ‘root’ account) when a non-privileged account will do.

3.4.7 Services and applications that will not be used must be disabled where practical.

3.4.8 Access to services shall be logged and/or protected through access-control methods such as TCP wrappers, if possible.

3.4.9 Trust relationships between systems are a security risk, and their use shall be avoided. Do not use a trust relationship when some other method of communication will do.

3.4.10 All security-related events on critical or sensitive systems shall be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week
- Daily incremental tape backups will be retained for at least 1 month
- Weekly full tape backups of logs will be retained for at least 1 month
- Monthly full backups will be retained for a minimum of 1 year

3.4.11 Security-related events shall be reported to SMD-IPQS who shall review logs and report incidents to the Deputy Commissioner of the Information Systems Group (DCIR-ISG). Corrective measures shall be prescribed as needed. Security-related events include, but are not limited to:

- Port scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

3.5 Intranet Security Policies

3.5.1 The Bureau’s intranet shall be intended to facilitate more efficient and more effective ways for Bureau’s personnel to communicate and conduct business.

3.5.2 Before any information is posted to the Bureau’s intranet, it should be approved by the Division Chief in-charge of the relevant intranet web page and the owner of the involved information. Unless approved in advance by the Assistant Commissioner of the Information Systems Development Service (ACIR-ISDS), and explicitly noted on the intranet page in question, all contents posted to the intranet shall be property of the Bureau.

3.5.3 All third party access to Bureau’s internal computer systems which are not clearly public (such as the intranet) shall be approved by SMD-IPQS.

3.5.4 The Bureau’s intranet is for the exclusive use of authorized personnel. Employees must not forward information appearing on the intranet to third parties without going through the appropriate internal channels (SSD, IPQS, DCIR-ISG).
3.6  Internet Security Policies

3.6.1 The Bureau’s internet facility shall only be used for official activities.

3.6.2 Access to the internet shall only be granted to authorized users as stated in RMO 29-2000: Policies and Guidelines on the Use and Maintenance of the Bureau’s E-mail and Internet Browsing Facilities.

3.6.3 Downloading of evaluation/unlicensed software is prohibited unless the proper authorization duly noted by a higher Bureau’s official of the concerned service or group and approved by the DCIR-ISG.

3.6.4 Users should assume that all materials on the internet are copyrighted unless specific notice states otherwise.

3.6.5 Users shall not save permanent passwords in their web browsers because this may allow anybody who has physical access to their workstations to access the Internet with their identities.

3.6.6 Unless approved by the DCIR-ISG, users must not establish internet or other external network connections that could allow unauthorized users to gain access to Bureau's systems and information.

3.6.7 Unauthorized internet hosting is strictly prohibited.

3.6.8 Users using Bureau’s resources must not connect/surf to websites that contain sexually explicit, racist, violent, or other potentially offensive material.

3.6.9 Use of Chat Software / Electronic Chat such as Internet Relay Chat (IRC), I Seek You (ICQ), Yahoo/MSN Messenger and other forms of real-time communication software and devices which makes use of the internet and its related technologies as well as on-line internet games are strictly prohibited.

3.6.10 Use of information systems to access internet for unauthorized purposes shall not be tolerated and may be considered cause for disciplinary action up to and including termination.

3.6.11 When users provide information on public forums such as chat sessions, bulletin boards, etc., they must also clearly indicate that the opinions expressed are their own and not necessarily those of BIR.

3.6.12 BIR reserves the right to block access to sites deemed inappropriate.

3.6.13 Users of BIR’s Internet connection should realize that their communications are not automatically protected from viewing by third parties. Unless encryption and/or other approved security practices are employed, users shall not send/post information if they consider it to be private and/or confidential.

3.6.14 Users are reminded that Web browsers leave “footprints” (or cookies) providing a trail of all site visits.

3.6.15 BIR may keep logs and serves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks and cookies, logs of web sites visited, and other information stored on or passing through BIR computers.

3.6.16 DCIR-ISG shall approve the establishing of new business arrangements via the Internet (e.g Electronic Data Interchange (EDI) arrangements).
3.6.17 All software used to access the World Wide Web must be approved by the Network Administrator and must incorporate all appropriate/approved vendor provided security patches.

3.6.18 Access to internal services from the Internet shall be via a secure (encrypted) login process. Subsequent transactions processes shall be secure as well.

3.6.19 The use of telnet connection with fixed passwords over the Internet shall be prohibited.

3.6.20 All connections to and from the Internet shall authenticate through a corporate approved firewall. Individual Internet Service Provider (ISP) accounts (i.e. AOL) and individual dial-up lines to access the internet via BIR’s systems shall not be allowed. This precludes “dialing around the company’s Internet connection” or dialing into a computer from within the company (i.e. pcAnywhere).

3.6.21 Sensitive, confidential, and private information shall never be stored on servers and/or shares where unauthenticated access is permitted to the public (Internet).

3.6.22 Documentation, software, and other intellectual property must not be sold or otherwise transferred to any non BIR user unless specific and adequate terms and conditions are implied.

3.6.23 Inappropriate electronic postings, which include non-work related postings, to public forums are prohibited. Management reserves the right to remove these and other postings which are inconsistent with BIR’s business interests and/or existing policy statements. DCIR-ISG shall approve the posting of BIR material on the Internet prior to posting.

3.6.24 Security credentials, such as logins and passwords shall only be sent via the Internet through secured, encrypted means. Management must approve other processes.

3.6.25 ACIR-ISDS shall approve all web pages hosted on BIR owned or operated systems.

3.6.26 Any file downloaded over the World Wide Web shall be scanned for viruses, using approved virus detection software.

3.6.27 All representations on behalf of BIR must first be cleared by management. In addition, users shall not release company information or enter into any transactions such as contracts and including placing orders, until the identity of the individual and organization contacted are confirmed.

3.6.28 Users shall not misrepresent or falsify their identity on the Internet or in any BIR communications. In official company communications, the user’s name, organization and other company specific information shall be included in the message or posting.

3.6.29 Copying of software in a manner that is not consistent with the vendor’s license is strictly forbidden. All licensed software shall be monitored and controlled by the Systems Support Division of ISOS, likewise, installation and update of software shall be done by personnel of said group.

3.6.30 All publicly writable directories where authentication is not required (i.e. anonymous FTP) will be deleted on a nightly basis to prevent the anonymous exchange of information inconsistent with BIR’s business.

3.6.31 If sensitive, confidential, and/or private information is or is suspected to be lost or disclosed to unauthorized parties, the SMD-IPQS shall be notified immediately.
3.6.32 If unauthorized use of BIR information system has taken place or is suspected, the SMD-IPQS shall be notified immediately.

3.6.33 All unusual systems behavior, such as missing files, frequent system crashes misrouted messages, and other similar activities occur, the SSD-ISOS shall be notified immediately.

3.6.34 The specifics of any possible security problems shall be kept confidential to immediate management and security personnel.

3.6.35 Users shall not test security mechanisms at either BIR or other Internet sites, nor use and/or possess tools for cracking information security unless express written permission is obtained.

3.7. Extranet Policies

3.7.1 All new extranet connectivity shall go through a security review with the SMD-IPQS. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

3.7.2 All new connection requests between third parties and BIR require that the third party and the Bureau representatives agree to and sign the Non Disclosure Agreement (Annex D). This agreement must be signed by the Chief of Security Management Division and the DCIR, ISG as well as a representative from the third party who is legally empowered to sign on behalf of the third party. Documents pertaining to connections into BIR labs are to be kept on file by SSD-ISOS.

3.7.3 All production extranet connections shall be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Lab connections must be approved by the SSD-ISOS. Typically, this function is handled as part of the Third Party Agreement.

3.7.4 The Sponsoring Organization must designate a person to be the Point of Contact for the Extranet connection. The point of contact acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy. In the event that the Point of Contact changes, the relevant extranet organization must be informed promptly.

3.7.5 The Sponsoring Organization within the Bureau who wishes to establish connectivity to a third party shall file a new site request with the proper extranet group. The extranet group will engage SMD-IPQS to address security issues inherent in the project. If the proposed connection is to terminate within a lab at BIR, the Sponsoring Organization must engage the SMD-IPQS. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and SMD-IPQS, as requested.

3.7.6 In general, services provided over Third Party Network Connections should be limited only to those services needed, and only those devices (hosts, routers, etc.) needed. Blanket access will not be provided for anyone.

The standard set of allowable services are:

- File Exchange via ftp
- Electronic Mail Exchange
- Web Resource Access
- Print Services
- NT File Exchange
3.7.7 The SSD-ISOS and/or SMD-IPQS shall be responsible for the installation and configuration of a specific Third Party Connection and must ensure that all possible measures have been taken to protect the integrity and privacy of BIR confidential information. At no time should BIR rely on access/authorization control mechanisms at the Third Party's site to protect or prohibit access to Bureau's confidential information.

3.7.8 In no case shall a Third Party Network Connection to BIR be used as the Internet connection for the Third Party.

3.7.9 All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the SSD-ISOS and/or SMD-IPQS when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

3.7.10 When access is no longer required, the Sponsoring Organization within BIR must notify the extranet team responsible for that connectivity, which will then terminate the access. The extranet and lab security team must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct the Bureau business, will be terminated immediately. Should a security incident or a finding that a circuit has been depreciated and is no longer being used to conduct BIR business necessitate, a modification of existing permissions, or termination of connectivity, SMD-IPQS and/or the extranet team will notify the Point of Contact or the Sponsoring Organization of the change prior to taking any action.

3.7.11 Enable-level access to BIR-owned/maintained equipment on the Third Party premise will only be provided to the appropriate support organization. All other business personnel will have restricted access/read-only access to the routers at their site and will not be allowed to make configuration changes.

3.7.12 The Bureau shall not have any responsibility for ensuring protection of Third Party information. The Third Party shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.

3.8 Wireless Communication / Mobile Tele-Working Policies

3.8.1 The Bureau shall maintain point to point hardware encryption of at least 56 bits.

3.8.2 The Bureau shall maintain a hardware address that can be registered and tracked (i.e. a MAC Address).

3.8.3 The Bureau shall support strong user authentication which checks against an external database such as TACACS, RADIUS or something similar.

3.9. Virtual Private Network (VPN) Policies

3.9.1 It is the responsibility of the Network Administrator to ensure that unauthorized users are not allowed access to the Bureau’s Internet networks.

3.9.2 VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

3.9.3 When actively connected to the network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.
3.9.4 Dual (split) tunneling is NOT permitted; only one network connection is allowed.

3.9.5 VPN gateways will be set up and managed by the network group of Information Systems Operation Service (SSD-ISOS).

3.9.6 All computers connected to BIR internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

3.9.7 Users with VPN connectivity shall be automatically disconnected from the Bureau’s network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

3.9.8 The VPN concentrator is limited to an absolute connection time of 24 hours.

3.9.9 Users of computers that are not BIR-owned equipment must configure the equipment to comply with the Bureau’s VPN and network policies.

3.9.10 Only SMD-IPQS approved VPN clients may be used.

3.9.11 By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the Bureau’s network, and as such are subject to the same rules and regulations that apply to BIR-owned equipment, i.e. their machines must be configured to comply with the Bureau’s security policies.

3.10. Firewall Security Policies

3.10.1 All internet connectivity path and internet services must pass through firewalls for security, control and restrictions.

3.10.2 Firewall back-up files must be kept close to the server at all times.

3.10.3 Firewalls must only run on dedicated machines.

3.10.4 All firewall servers must be placed in a physically secured area accessible only to authorized personnel.

3.11 Internet DMZ Equipment Policies

3.11.1 Hardware, operating systems, services and applications shall be approved by SSD-ISOS as part of the pre-deployment review phase.

3.11.2 Operating system configuration must be done according to the secure host and router installation and configuration standards.

3.11.3 All patches/hot fixes recommended by the equipment vendor and SMD-IPQS must be installed. This applies to all services installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hot fixes.

3.11.4 Services and applications not serving business requirements must be disabled.

3.11.5 Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by SSD-ISOS.

3.11.6 Services and applications not for general access must be restricted by access control list.
3.11.7 Insecure Services or protocols must be replaced with more secure equivalents whenever such exist.

3.11.8 Remote administration must be performed over secure channels (e.g. encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

3.11.9 All host content updates must occur over secure channels.

3.11.10 Security-related events must be logged and audit trails saved to SMD-IPQS approved logs. Security-related events include (but are not limited to) the following:

- User login failures
- Failure to obtain privileged access
- Access policy violations

3.11.11 SMD-IPQS shall address non-compliance waiver requests on a case-to-case basis and approve waivers if justified.

3.11.12 Configuration changes must follow the Change Management Procedures.

3.11.13 SMD-IPQS shall be invited to perform system/application audits prior to the deployment of new services.

3.11.14 SMD-IPQS shall be engaged, either directly or via Change Management, to approve all new deployments and configuration changes.


3.12.1 Database accounts shall integrate authentication with the operating system. Non-technical users shall have no direct access to the operating system shell. A menu-driven facility shall be made available to non-technical users.

3.12.2 Access privileges of users shall be on a role-based scheme wherein users have access to resources based on the user’s role. Access rights shall be grouped by role/job designation, and access to resources is restricted to users who have been authorized to assume the associated role/job designation. Each user may be assigned one or more roles, and each role may be assigned one or more access privileges.

3.12.3 Any request for creation of database link on productions server shall require approval of SMD-IPQS.

3.12.4 All necessary and updated patches shall be applied for any discovered critical security vulnerabilities affecting the database (e.g. buffer overflow vulnerabilities for create database link queries).

3.12.5 User shall not be allowed to grant, in any manner, his/her existing system privilege to a role or other users without the approval of DCIR-ISG

3.13. Dial-In Access Policy

3.13.1 BIR employees and authorized third parties (customer, vendors, etc.) can use dial-in connection to gain access to the corporate network. Dial-in access should be strictly controlled, using one-time password authentication.
3.13.2 It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to BIR is not used by non-employees to gain access to company information system resources.

An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and the Bureau are literal extensions of BIR's corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect the Bureau's assets.

3.13.3 Analog and non-GSM digital cellular phones cannot be used to connect to the Bureau's corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to BIR's network.

Note: Dial-in accounts are considered “as needed” accounts for BIR. Account activity is monitored, and if a dial-in account is not used for a period of six months the account will expire and no longer function. If a dial-in access is subsequently required, the individual must request a new account.


3.14.1 It is the responsibility of employees, contractors, vendors and/or solution provider with remote access privileges to Bureau’s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

3.14.2 Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.

3.14.3 At no time should any employee provide their login or email password to anyone, not even family members.

3.14.4 Employees and third party with remote access privileges must ensure that their Bureau-owned or personal computer or workstation, which is remotely connected to Bureau's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

3.14.5 Employees and third party with remote access privileges to Bureau's corporate network must not use non-Bureau email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Bureau's business to ensure that official business is never confused with personal business.

3.14.6 Routers for dedicated ISDN lines configured for access to the Bureau's network must meet minimum authentication requirements of CHAP (Challenge Handshake Authentication Protocol).

3.14.7 Non-standard hardware configurations must meet approved Remote Access Services, and SMD-IPQS must approve security configurations for access to hardware.

3.14.8 All hosts that are connected to Bureau’s internal networks via remote access technologies must use the most up-to-date anti-virus software.

3.14.9 Personal equipment that is used to connect to Bureau's networks must meet the requirements of Bureau-owned equipment for remote access.
3.15. Analog/ISDN Line Security Policies

3.15.1 Fax lines are to be approved for office use only.

3.15.2 No fax lines shall be installed for personal use.

3.15.3 No analog lines shall be placed in a personal cubicle.

3.15.4 The fax machine shall be placed in a centralized administrative area and away from other computer equipment.

3.15.5 A computer which is capable of making a fax connection shall not be allowed to use an analog line for this purpose.

3.15.6 Requests for computers or other intelligent devices to be connected with analog or ISDN lines from within the Bureau will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to BIR, and active penetrations have been launched against such lines by hackers. Waivers to this policy will be granted by the DCIR-ISG on a case by case basis.

3.15.7 Once approved by the DCIR-ISG, any office requesting an analog/ISDN line must provide the following information to Telecom:

- A clearly detailed business case of why other secure connections available at the Bureau cannot be used.
- The business purpose for which the analog line is to be used.
- The software and hardware to be connected to the line and used across the line.
- And to what external connections the requester is seeking access.

3.16. Internal Lab Security Policies

3.16.1 All traffic between the corporate production and the lab network must go through a Network Support Organization (SSD-ISOS) maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production needed.

3.16.2 Original firewall configurations and any changes thereto must be reviewed and approved by SMD-IPQS. The SMD-IPQS may require security improvements as needed.

3.16.3 Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-BIR networks. These activities must be restricted within the lab.

3.16.4 Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

3.16.5 The SMD-IPQS reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls, and network peripherals.

3.16.6 Lab owned gateway devices are required to comply with all BIR product security advisories and must authenticate against the Bureau’s Authentication servers.
3.16.7 The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with the Bureau’s Password Policy.

3.16.8 In labs where non-BIR personnel have physical access, direct connectivity to the production network is not allowed. Connectivity for authorized personnel from these labs can be allowed to the Bureau’s production network only if authenticated against the authentication servers, temporary access lists (lock and key), SSH, client VPNs or other similar technology.

3.16.9 All lab external connection requests must be reviewed and approved by SMD-IPQS. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

3.16.10 All lab networks with external connections must not be connected to BIR production network or any other Internal network directly or via a wireless connection, or via other form of computing equipment. A waiver from SMD-IPQS is required where air-gapping is not possible (e.g. Partner Connections to third party networks).

3.17. DMZ Lab Security Policies

3.17.1 All new DMZ Labs shall present a business justification with sign-off at the Information Systems Operations Service (ISOS). SMD-IPQS must keep the business justifications on file.

3.17.2 Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ Labs must be requested through the Systems Support Division of the Information Systems Operation Service (SSD-ISOS) and approved by SMD-IPQS.

3.17.3 All ISP connections shall be maintained by the SSD-ISOS.

3.17.4 The SSD-ISOS shall maintain a firewall device between the DMZ Lab(s) and the Internet.

3.17.5 The SSD-ISOS and SMD-IPQS reserve the right to interrupt lab connections if a security concern exists.

3.17.6 The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to the SSD-ISOS point of demarcation.

3.17.7 The SSD-ISOS shall record all DMZ Lab address spaces and current contact information.

3.17.8 Individual lab accounts must be deleted within three (3) days when access is no longer authorized. Group account passwords must comply with the Password Policy and must be changed within three (3) days from a change in the group membership.

3.17.9 DMZ Labs must not be connected to the Bureau’s corporate internal networks, either directly or via a wireless connection.

3.17.10 All applicable security patches/hot fixes recommended by the vendor must be installed.

3.17.11 Services and applications not serving business requirements must be disabled.
3.17.12 Remote administration must be performed over secure channels (e.g. encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

3.17.13 All BIR PC-based lab computers must have the Bureau’s standard, supported anti-virus software installed.

3.17.14 Lab administrator is responsible for creating procedures that ensure anti-virus software is running at regular intervals, and computers are verified as virus free. In addition, the anti-virus software and the virus pattern files must be kept up-to-date.

3.18. Information Sensitivity Policies

- **Minimal Sensitivity:** General bureau/corporate information; some personnel and technical information

  Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "<Company Name> Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "<Company Name> Proprietary" or similar labels at the discretion of the individual business unit or office.

  **Access:** BIR employees, contractors, people with a business need to know.

  **Distribution within BIR:** Standard interoffice mail, approved electronic mail and electronic file transmission methods.

  **Distribution outside BIR internal Mail:** Public or private carriers, approved electronic mail and electronic file transmission methods.

  **Electronic Distribution:** No restrictions except that it be sent to only approved recipients.

  **Storage:** Keep from view of unauthorized people; do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

  **Disposal/Destruction:** Deposit outdated paper information in specially marked disposal bins on Bureau’s premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

  **Penalty for deliberate or inadvertent disclosure:** Up to and including termination, possible civil and/or criminal prosecution.

- **More Sensitive:** Business, financial, technical, and most personnel information

  **Access:** BIR employees and non-employees with signed non-disclosure agreements who have a business need to know.

  **Distribution within BIR:** Standard interoffice mail, approved electronic mail and electronic file transmission methods.

  **Distribution outside BIR internal mail:** Any approved private carrier.

  **Electronic Distribution:** No restrictions to approved recipients within the Bureau, but should be encrypted or sent via a private link to approved recipients outside of the Bureau’s premises.
Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on BIR premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

- Most Sensitive: Trade Secrets and marketing, operational, personnel, financial, source code, & technical information integral to the success of the BIR.

To indicate that Bureau confidential information is very sensitive, you should label the information “BIR Internal: Registered and Restricted”, “BIR Confidential” or similar labels at the discretion of the individual business unit or office. Users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (BIR employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within BIR: Delivered direct – signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of BIR internal mail: Delivered direct; signature required; approved private carriers.

Electronic Distribution: No restrictions to approved recipients within the Bureau, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strong encouraged: in specially marked disposal bins on BIR premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.


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

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

3.19.3 Naming standards shall support a single internal User-ID for all platforms (unless specific system precludes this option). Exceptions must be documented.

3.19.4 A User Agreement (Annex E) must accompany all requests for authorization or re-authorization of a new user-ID.

3.19.5 User accounts and passwords shall be distributed to employees in a secure manner. User accounts and passwords shall be distributed by telephone only after the employee has been authenticated.
3.19.6 Additional restrictions shall be placed on non-employee usernames and passwords including but not limited to audit and account policies.

3.19.7 Administrative/Super-User accounts shall be limited in number.

3.19.8 Service accounts must not be used for administrative activities.

3.19.9 Administrative/Super-Users shall maintain two accounts: one privileged for administrative functions and one normal end user account for day-to-day activities.

3.19.10 Passwords must be sufficiently complex (avoid names, places, birthdays, company slogans, dictionary words, etc) and include:

- The minimum password length employed on all accounts will be a minimum of 8 characters.
- The system shall require password changes at least a minimum of one (1) week and a maximum of thirteen (13) weeks.
- Passwords must contain both alphabetic and non-alphabetic characters (numeric or symbol).
- Passwords must allow both upper and lowercase characters.
- Password history shall be kept for at least 5 previous passwords.
- The minimum password age shall be set at 2 days to regulate the automatic reuse of old passwords and to allow for potentially compromised passwords to be changed quickly.

3.19.11 Users shall be forced to change their password upon initial use/receipt and upon password reset.

3.19.12 Users shall change their passwords immediately if it is believed that the password has been compromised.

3.19.13 Users of BIR shall not ask for, or provide password disclosure for any account managed by BIR systems.

3.19.14 Writing of passwords and leaving them where others could discover them is strictly prohibited.

3.19.15 All default passwords provided by software or hardware must be changed once implemented on production systems or development systems attached to the network or Internet.

3.19.16 Fixed plain text passwords embedded in software or scripts shall not be used on production systems or development systems attached to the network or Internet.

3.19.17 Users and Administrators who maintain multiple accounts must use different passwords on each of the accounts.

3.19.18 Administrator accounts shall require password changes at least a minimum of every 7 days.

3.19.19 User of emergency operations/fire call passwords will be strictly controlled and approved by management.

3.19.20 A user-ID and password are required for access to the network and computer systems. Anonymous User-IDs will not be allowed. Servers supporting the use of anonymous ftp may be authorized but will be isolated from internal networks and systems.
3.19.21 The limit on consecutive unsuccessful access attempts will be limited to 3 within a 60-minute timeframe. Once locked out, only the System Administrator can unlock the account.

3.19.22 Successful logons shall display the date and time of the last logon to the user.

3.19.23 Users shall not leave a terminal that has an active logon session connected to it unattended and unprotected.

3.19.24 User-IDs shall be suspended after a specific period of inactivity.

3.19.25 User password must not be scripted nor hardcoded (i.e. placed in a function key, macro, or using “Save Password on next connect”).

3.19.26 Incorrect login information shall not be displayed to end-users.

3.19.27 A security notice banner shall be displayed to end users at each login.

3.20. User Account Management Policies

3.20.1 An Access request form requiring a user’s immediate supervisor or manager sign-off will form the basis of all formal requests for access to all multi-user IT services.

- Request for System Access Form (Annex F)
- eFPS Access Request Form (Annex G)

3.20.2 A user’s immediate supervisor or manager is responsible for reporting changes in user duties that impact the need to access information or systems.

3.20.3 The following scenarios shall require user to file a Revocation of Access (Annex H):

- ITS user ends service to BIR
- ITS user is suspended from work
- ITS user goes on an extended leave
- Change in location, permanent transfer

3.20.4 The SMD-PQS shall periodically validate user accounts and privileges. Any inactive accounts shall be disabled and removed after a period of one month.

3.20.5 Accountability and traceability to individuals shall be maintained for all privileged system commands/actions on critical systems.

3.20.6 Users shall be notified that their actions may be monitored and recorded when using BIR systems.

3.20.7 Users shall not use any other user’s account with or without that user’s permission.

3.20.8 Logging of privileged account actions and relevant security events shall be employed on all systems including sufficient data to support security audits (e.g. user logon information, access to privileged resources, and changes to production information).

3.20.9 Audit logs containing security relevant events must be retained off-line for a period of one year.

3.20.10 Audit logs on the most critical systems shall be resistant to attacks including attempts to deactivate, modify, or delete the logging software and/or the logs themselves.
3.20.11 Mechanisms for time synchronization for accurate logging of events on the network shall be employed and managed.

3.20.12 Monitoring of static web pages shall be employed to ensure that web page defacement attempts are corrected in real-time.

3.20.13 The SMD-IPQS shall review audit logs as necessary to identify possible system or data compromise. In addition, security audits (including the use of automated tools) will be used as appropriate to monitor compliance with security policies.

3.21 Acceptable Use of Computer Equipment Policies

3.21.1 While the Bureau desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the Bureau. Because of the need to protect the Bureau’s network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Bureau.

3.21.2 Employees shall be responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such policies, employees should be guided by the Bureau’s policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3.21.3 Security Management Division, IPQS (SMD-IPQS) shall recommend that any information that users consider sensitive or vulnerable be encrypted.

3.21.4 Adding of Personal Computer (PC) or laptop to the network shall be directly reported to the Systems Support Division of Information Systems Operations Service (SSD-ISOS)

3.21.5 For security and network maintenance purposes, the Systems Support Division of Information Systems Operations Service (SSD-ISOS) shall monitor equipment, systems, and network traffic at any time.

3.21.6 Systems privileges of all users, systems and standalone programs must be restricted on a need-to-know basis. Privileges must not be extended unless a legitimate business-oriented need for such privilege exists and has been approved accordingly.

3.21.7 The user interface for information contained on internet, intranet, and extranet-related systems should be classified as either confidential or not confidential.

3.21.8 All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less, or by logging-off when the host will be unattended.

3.21.9 Changes in configuration and settings in all equipment shall only be done by authorized personnel of SSD-ISOS.

3.21.10 The Network Administrator shall maintain an inventory list of IP addresses of workstations connected to the Bureau’s network.

3.21.11 Printers shall be located in areas accessible to the system users so that they can easily obtain official printouts.

3.21.12 All printouts that remain unclaimed for 30 days shall be disposed, upon approval of the Head of Office, by shredding or by some other means as determined by the Head of Office.
3.21.13 Tapes/diskettes containing information for/from the database shall be secured under locks which are controlled by the Head of Computer Operations and Computer Librarian.

3.21.14 Only the Computer Librarian, Head of Computer Operations, and Systems Administrators are authorized to retrieve tapes and disks.

3.21.15 User encryption of information shall be in compliance with Acceptable Encryption Use policy.

3.21.16 It is a violation of this policy to disable any monitoring tool/facility installed on any system or network.

3.22. Acceptable Encryption Use Policies

3.22.1 Proven standard algorithms such as Data Encryption Standard (DES), Blowfish, RSA (Rivest, Shamir, Adleman), RC5 (Block Cipher Algorithm), and International Data Encryption Algorithm (IDEA) shall be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Symmetric crypto-system key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. The Bureau's key length requirements will be reviewed annually and upgraded as technology allows.

3.22.2 The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by SMD-IPQS.

3.23. Acquisition Assessment Policies

Acquisition assessments are conducted to ensure that equipment and systems acquired by BIR do not pose a security risk to corporate network, internal systems, and/or confidential/sensitive information. SMD-IPQS will provide personnel to serve as active members of the evaluation team. The role of the SMD-IPQS is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to the Bureau’s networks.

3.23.1 All hosts (servers, desktops, laptops) will be replaced or re-imaged with a BIR standard image.

3.23.2 Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by SMD-IPQS.

3.23.3 All PC-based hosts shall require Bureau-approved virus protection before the network connection.

3.23.4 All network devices shall be replaced or re-imaged with a BIR standard image.

3.23.5 When justified by business requirements, air-gapped Internet connections require SSD-ISOS review and approval.

3.23.6 Remote access to the production network shall be provided by the Bureau.

3.23.7 Lab equipment shall be physically separated and secured from non-lab areas.
3.23.8 The lab network must be separated from the corporate production network with a firewall between the two networks.

3.23.9 Any direct network connections (including analog lines, ISDN lines, T1, etc) to external customers, partners, etc, must be reviewed and approved by the network administrator.

3.23.10 All acquired labs shall meet with the lab security policy or be granted a waiver by the network administrator.

3.23.11 In the event the acquired networks and computer systems being connected to the corporate network fail to meet the requirements, the DCIR-ISG as per recommendation of the ACIR-IPQS must acknowledge and approve of the risk to the Bureau’s network.

3.24. Audit Policies

3.24.1 When requested, and for the purpose of performing an audit, any access needed will be provided to members of the SMD-IPQS.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Bureau equipment or premises
- Access to work areas (offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Bureau networks.

3.24.2 Database Administrators should continuously monitor/audit user access to sensitive objects as well as database actions.

3.24.3 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of one (1) week.
- Daily incremental tape backups will be retained for at least one (1) month.
- Weekly full tape backups of logs will be retained for at least one (1) month.
- Monthly full backups will be retained for a minimum of two (2) years.

During this period, such logs or backups must be secured such that they cannot be modified, and such that they can be read only by authorized Bureau personnel. Said logs are important for error correction, forensic auditing, security breach investigations, and any other related efforts.

3.25. Risk & Vulnerability Assessment / Penetration Testing Policy

The conduct of RVA and Penetration Testing shall only be done by SMD-IPQS in coordination with the office responsible for the systems area being assessed. Employees are expected to cooperate fully with any RVA and Pen Test being conducted on systems for which they are not held accountable. Employees are further expected to work with the SMD-IPQS Risk Assessment Team in the development and implementation of a remediation plan.


3.26.1 The Bureau shall reserve the right to periodically audit the application infrastructure of an outsourcing company employed by the Bureau to ensure compliance with the herein stated policies. Non-intrusive network audits (basic port scan, etc.) may be
done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.

3.26.2 All network configuration requirements of third parties shall be put into writing and coursed through the Chief of the Network Group and approved by the Assistant Commissioner of Information Systems & Operations Service (ACIR-ISOS) prior to implementation in production.

3.26.3 The contractor shall submit an architecture document that includes a full network diagram of the application environment, illustrating the relationship between the environment and any other relevant networks, with a full data flowchart that details where the project’s data resides, the applications that manipulate it, and the security thereof.

3.26.4 The contractor shall be able to immediately disable all or part of the functionality of the application should a security issue be identified.

3.26.5 The equipment hosting the application (whether outsourced or a P.O.C.) must be located in a physically secured facility.

3.26.6 The Bureau shall have the final say on who shall be authorized to enter any locked physical environment, as well as access the Application Infrastructure. Contractors shall be allowed to stay inside a restricted area only when accompanied by BIR personnel.

3.26.7 The contractor shall disclose who amongst their personnel shall have access to the environment hosting the application for the Bureau.

3.26.8 The network hosting the application must be air-gapped from any other network or customer that the contractor/provider may have. This means their application environment must use separate hosts, and separate infrastructure.

3.26.9 Relative to the data flow between the Bureau and the contractor/provider, the following should be observed:

- If the contractor will be connecting to the Bureau via a private circuit (such as frame relay, etc.), then that circuit must terminate on their extranet, and the operation of that circuit will come under the procedures and policies that govern Bureau networks.

- If, on the other hand, the data between Bureau and the contractor will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the contractor, and the traffic in-between must be protected and authenticated by cryptographic technology.

3.26.10 The contractor shall provide listing of current patches on hosts, including host (OS) patches, web servers, databases, and other material application. Information on how and when security patches will be applied shall also be provided.

3.26.11 The contractor shall disclose the process for monitoring the integrity and availability of hosts mentioned in 3.26.9.

3.26.12 Application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community. Connections utilizing the internet must be protected of cryptographic technologies (i.e. IPSec, SSL, SSH/SCP, PGP).
3.26.13 In the event that BIR data or applications are to be manipulated by, or hosted at, a contractor’s service, it must have a written explicit permission from the data/application owners.

3.27. Third Party Information Disclosure Security Policies

3.27.1 Taxpayer’s information must be protected from unauthorized disclosure to third parties.

3.27.2 All requests for Bureau’s information must be accompanied with a written justification from the third party.

3.27.3 The contractor must disclose how and to what extent the hosts (Unix, NT, etc.) comprising their application infrastructure have been hardened against attack. Hardening documentation must be provided as well, if available.

3.27.4 Information relative to Bureau’s IT infrastructure can be released to a third party provided:
- 3.27.4.1 Release of such information has been approved by DCIR-ISG, and
- 3.27.4.2 A Non-Disclosure Agreement has been signed by recipient of information.

3.27.5 If any “confidential” information has been inappropriately disclosed, this must be reported to the Head of Office and the person who disclosed the information must be dealt with according to the provisions of RMO 50-98: Implementing the Updated Code of Conduct for Bureau of Internal Revenue Officers and Employees.

3.27.6 Records of disclosures referred to in item 3.24.3 should be documented and reported to SMD-IPQS.

4. RESPONSIBILITIES

4.1 SECURITY MANAGEMENT DIVISION, INFORMATION PLANNING AND QUALITY SERVICE (SMD-IPQS)

SMD-IPQS shall be responsible for establishing, maintaining, and administering organization-wide Information and Communications Technology security policies, standards, guidelines and procedures. SMD shall therefore be responsible for activities related to these policies in close coordination with the Network and System Administrators such as:

- Information systems risk assessment
- Preparation of information systems security action plans
- Evaluation of information security products
- Conduct of investigations into any alleged computer or network security compromises, incidents or problems

4.2 NETWORK / SYSTEMS ADMINISTRATORS

Network and Systems Administrators of both the SSD-ISOS and the Revenue Data Centers shall:

- Act as information security coordinators and implement appropriate user privileges, monitor access/system control logs on their areas of responsibility,
- NO Network Administrators for NO network infrastructure (NO Bldg, Revenue Computer Center Bldg and TIN Building)
• Revenue Data Center Network Administrators for RDC, RR and RDO network infrastructure
• Be responsible for reporting all suspicious computer and network-security-related activities to SMD-IPQS. Whenever system security has been compromised, or even if there is a justifiable reason to believe it has been compromised, the Systems/Network Administrator concerned must immediately do any or all of the following:
  • reassign all relevant passwords;
  • force every password on the involved system to be changed at the time of the next login. If this is not possible, a broadcast message must be sent to all users instructing them to change their passwords;
  • immediately review all changes to user privileges taking effect since the time of suspected compromise for any unauthorized modifications.
• Serve as local information security liaisons, implementing the requirements of this and other information system security policies, standards, guidelines and procedures.

4.3 DATABASE ADMINISTRATORS

Database Administrators of both development and production shall:

• Act as information security coordinators and implement appropriate user privileges, monitor access/system control logs on their areas of responsibility.
• Be responsible for reporting all suspicious database-security-related activities to SMD-IPQS. Whenever database security has been compromised, or even if there is a justifiable reason to believe it has been compromised, the concerned Database Administrator concerned must immediately do any or all of the following:
  • reassign all relevant passwords;
  • force every password on the involved system to be changed at the time of the next login. If this is not possible, a broadcast message must be sent to all users instructing them to change their passwords;
  • Immediately review all changes to user / object privileges taking effect since the time of suspected compromise for any unauthorized modifications.
• Serve as local information security liaisons, implementing the requirements of this and other information system security policies, standards, guidelines and procedures.

4.4 DIVISION CHIEFS / HEADS OF OFFICES

All Division Chiefs / Heads of Offices shall be responsible for ensuring that appropriate Information and Communications Technology security measures are observed in their respective areas. They shall also be responsible for ensuring that all users within their respective divisions are aware of and compliant to the Bureau’s security policies.

4.5 USERS

Users shall be responsible for complying with the herein stated policies and all other Bureau policies defining computer and network security measures. Violations to said policies and associated procedures shall be reported and be dealt with according to the provisions of RMO 50-98.