



BUREAU OF CUSTOMS

MAKABAGONG ADUANA, MATATAG NA EKONOMIYA



PROFESSIONALISM

INTEGRITY

ACCOUNTABILITY

Date: 12.21.2021

CUSTOMS MEMORANDUM ORDER (CMO)

NO. 01-2022

SUBJECT: BUREAU OF CUSTOMS INFORMATION SECURITY POLICY

Introduction. The Bureau of Customs (Bureau) processes and maintains information, in any form, that is classified in nature and must be protected against unauthorized access and disclosure. The confidentiality, integrity, and availability of information, in all its forms, are considered vital to the ongoing operations of the Bureau. Efficient management of such assets is also necessary to comply with the legal and regulatory requirements of the country. Failure to adequately secure information increases the risk of loss to revenue collection, reputational losses, and possible violation of existing laws.

This Information Security Policy aims to define the security requirements for the proper and secure use of the information-related services provided by the Bureau. This policy is a set of rules issued by the Bureau to ensure that all users, who are given access to its technology and information assets within its domain or network, comply with the guidelines and rules related to the security of the information stored digitally at any point in the network, domain, or within the Bureau's boundaries of authority.

For easy reference, a Topic Index is attached as **Annex A**.

Section 1. Objectives. The objectives of this policy are to:

- 1.1.** Provide a framework for establishing suitable levels of information security for all the Bureau's Information Systems (including, but not limited to, all Cloud environments, servers, computers, storage, mobile devices, networking equipment, software, and data) and to mitigate the risks related with the abuse, damage, loss, misuse, and theft of these systems.
- 1.2.** Ensure that all users understand their responsibilities for protecting the confidentiality, integrity, and availability of the data or information that they handle.
- 1.3.** Provide the principles by which safe and secure information systems working environment can be established for officers and employees of the Bureau.

Section 2. Scope. This Information Security Policy Manual applies to all officers and employees of the Bureau, including temporary users, visitors, contractors, service providers, and partners with granted clearances to have access to the Information Technology (IT) Systems and with limited or unlimited access time to different services and documents containing IT-related information. The information policy, procedures, guidelines, and best practices will apply to all groups, services, and divisions of the Bureau and it will govern all aspects of hardware, software, communications, and information. Compliance with the policies contained in this manual shall be mandatory for all persons engaged with the Bureau.

Section 3. Personnel Security. All personnel who manage or use the Bureau’s information systems shall have information security responsibilities, including, but not limited to, the following:

Roles	Responsibilities
Deputy Commissioner, Management Information Systems and Technology Group ("MISTG")	<ul style="list-style-type: none"> • Act as Chief Information Security Officer. • Accountable for all aspects of the Bureau’s IT-related security.
IT Security Officers (MISTG)	<ul style="list-style-type: none"> • Responsible for the security of the IT infrastructure and systems. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain specific security policy procedures. • Recommend timely and relevant security training programs. • Ensure that IT infrastructure and systems support security policies. • Respond to information security breach incidents and submit reports thereon. • Help in disaster recovery plans. • Provide employee information security reminders regularly. • Perform security audits. • Perform other functions as directed by the Chief Information Security Officer.
Chiefs of Divisions (Bureau-wide)	<ul style="list-style-type: none"> • Help with the security requirements for their specific area. • Provide and recommend physical and procedural safeguards. • Determine the privileges and access rights to the resources within their respective areas.

	<ul style="list-style-type: none"> • Determine a data retention period for the information, based on appropriate legal laws.
IT Security Team (MISTG)	<ul style="list-style-type: none"> • Implement and operate IT security. • Implement the privileges and access rights to the resources. • Support Security Policies. • Manage Incidents of Data Breach.
Users (Bureau-wide)	<ul style="list-style-type: none"> • Comply with all the Information Security Policies and all other controls established by Information Owners and Information Security Officers. • Access information only in support of their authorized job responsibilities. • Report any attempted security breaches. • Keep personal authentication devices (e.g., access cards, proximity cards, passwords, pins, etc.) confidential. • Initiate corrective actions when problems are identified.

Section 4. General Policy. All IT services should be used in compliance with the technical and security requirements defined in the design of the services.

Section 5. Exceptions to Policies. Exceptions to the policies defined in any part of this document may only be authorized by the Chief Information Officer or Information Security Officer, or as may be otherwise provided by law, rules or regulations. In those cases, specific procedures may be put in place to handle requests and authorizations for exceptions. Every time a policy exception is invoked, an entry must be entered into a security log specifying the date, time, description, reason for the exception, and how the risk was managed, or a request for exception letter must be provided.

Section 6. Policies.

6.1. IT Assets Acceptable Use Policy.

6.1.1. Purpose. The IT Assets Policy section defines the requirements and outlines the acceptable, proper, and secure use of all the IT assets in the Bureau to protect the latter and its employees. Inappropriate use exposes the Bureau to risks including virus attacks, compromise of network systems and services, and legal issues.

6.1.2. Scope. The policy applies to desktops, laptops, printers, copiers, networking equipment (switches, routers, access points, and servers), desk phones and other equipment/hardware owned or leased by the Bureau, to applications and software, to anyone using those assets, including internal users, temporary workers and visitors, and in general, to any resources and capabilities involved in the provision of the IT services. All employees,

contractors, consultants, and service providers are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources in accordance with the Bureau's policies and standards and local laws and regulations. Exceptions to this policy are documented in Section 6.1.4 (b).

6.1.3. Policy Definitions.

a. General Use and Ownership.

- i.** IT assets must only be used in connection with the business activities they are assigned and/or authorized.
- ii.** Every user is responsible for the preservation and correct use of the IT assets which they have been assigned.
- iii.** Every user shall have a responsibility to promptly report the theft, loss, or unauthorized disclosure of the Bureau's proprietary information.
- iv.** Every user may access, use, or share the Bureau's proprietary information provided that it is authorized and necessary to fulfill their assigned duties.
- v.** All the IT assets must be in locations with security access restrictions, environmental conditions, and layout according to the security classification and technical specifications of the assets.
- vi.** Employees are responsible for exercising good judgment regarding the reasonableness of personal use of Internet/Intranet/Extranet systems. Individual departments are responsible for creating guidelines concerning the personal use of the afore-mentioned. In the absence of such policies, employees should be guided by the departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

- vii.** For security and network maintenance purposes, authorized individuals within the Bureau may monitor equipment, systems, and network traffic, as may be deemed necessary, provided that the users of this equipment, systems, and network traffic have been notified of the purposes and limitations of such monitoring and maintenance activities, and have given their consent.
- viii.** Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approval of the proper authority.
- ix.** All personnel interacting with the IT assets must be equipped with proper training.
- x.** Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink nor eat near the equipment.
- xi.** Access to assets in the Organization's location must be restricted and properly authorized, including those accessing it remotely. The company's laptops, mobile devices, and other equipment used at the external location must be periodically checked and maintained, provided that the users of these laptops, mobile devices, and other equipment have been notified of the purposes and limitations of such periodic checks and maintenance, and have given their consent.
- xii.** The IT Technical Teams are solely responsible for maintaining and upgrading configurations. No other users are authorized to change or upgrade the configuration of the IT assets which includes modifying hardware or installing software.
- xiii.** Special care must be taken for protecting laptops, mobile devices, and other portable assets from being stolen. Users must be wary of extreme temperatures, magnetic fields, and falls.

- xiv.** When traveling by plane, portable equipment, like laptops and mobile devices, must remain in the possession of the user and carried as hand luggage.
- xv.** Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they were stolen.
- xvi.** Loss, theft, damage, tampering, or other incident related to assets, which compromises security, must be reported as soon as possible to the Information Security Officer.
- xvii.** IT Support shall conduct a periodic assessment of IT Assets to verify their status (i.e., in use/not use, functioning/nonfunctioning), provided that the users of these IT Assets have been notified of the purposes and limitations of the periodic assessment, and have given their consent. Appropriate action must be done by the IT Support (i.e., reissue, repair, disposal, etc.).
- xviii.** Disposal of the assets must be done according to specific procedures for the protection of the information stored therein. Prior to destruction/disposition of the assets, confidential information stored therein must be completely erased in the presence of an Information Security Team member. In addition, physical destruction must also be done in the presence the latter.

b. Security and Propriety Information.

- i.** System-level and user-level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure an access, is prohibited.
- ii.** Active desktops and laptops must be secured, if left unattended. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Every user must lock the screen or log off when the device

is unattended. Whenever possible, this policy should be automatically enforced.

- iii. Postings made by employees using the Bureau's email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Bureau, unless posting is in the course of official duties.
- iv. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

c. Unacceptable Use. The following activities are prohibited. However, employees may be exempted from these restrictions provided that they have authorized approval from the Chief Information Officer during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services).

The lists below are by no means exhaustive but attempts to provide a framework for activities that fall into the category of unacceptable use.

Also, reference to CMO No. 34-2015¹ may be made for additional IT Assets Usage Offenses and its equivalent administrative offense.

i. System and Network Activities. The following activities are strictly prohibited:

- 1. Violation of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Bureau.

¹ CMO No. 34-2015 entitled, "Use of Bureau of Customs Information and Communications Technology (ICT) Assets, Data, Information, and Network/Internetworking and Intranetworking Facilities.

2. Unauthorized copying of copyrighted material, including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, music, and the installation of any software, for which the Bureau or the end-user does not have an active license.
3. Accessing data, server, or an account for any purpose, other than conducting the Bureau's businesses, even with authorized access.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing the user's account password to others, or allowing the use thereof by others. This includes family and other household members when work is being done at home.
6. Using a Bureau's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any of the Bureau's account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but not limited to, network sniffing, pinged floods, packet spoofing, denial of service,

and forged routing information for malicious purposes.

9. Port scanning or security scanning is prohibited unless prior notification to IT Security Team is made.
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
11. Circumventing user authentication or security of any host, network, or account.
12. Interfering with, or denying, the service to any user other than the employee's host (e.g., denial of service attack).
13. Using any program/script/command or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
14. Providing information about, or lists of, the employees to parties outside the Bureau.

6.2. Access Control Policy.

6.2.1. Purpose. The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure in the Bureau. Access controls are put in place to protect information by controlling who has the right to use different information resources and by guarding against unauthorized use.

6.2.2. Scope. This policy applies to all offices and employees of the Bureau, including temporary users, visitors with temporary access to services, and partners with limited or unlimited access time to services.

6.2.3. Policy Definitions.

- a.** Any system that handles valuable information must be protected with a password-based access control system.
- b.** Any system that handles confidential information must be protected, if capable, by a two-factor-based access control system.
- c.** A discretionary access control list must be in place to control the access to resources for different groups of users.
- d.** Mandatory access controls should be in place to regulate access by the process operator on behalf of users.
- e.** Access rights and privileges to the Bureau's Information Systems and Network Domains must be allocated based on the user's specific task and function, rather than his/her status or position.
- f.** Access Level Categories are:
 - i.** All Access - the highest level of user access account. Manages the access and levels of the privilege and standard access accounts. Has access to all data, functions, and modules of an information system.
 - ii.** Privilege - a user access account that has more special rights than a standard user. Has access to a number of data, functions, and modules of the information systems. In some cases, these special accounts are used for management and maintenance information systems.
 - iii.** Standard - a basic user access account used for everyday tasks.
- g.** The creation of user access accounts with special privileges, such as administrators, must be rigorously controlled and restricted to only those users who are responsible for the management or maintenance of the information system or network. Each administrator must have a specific admin-level account, which is only used for system administration

purposes and is kept separate from their standard user access accounts.

- h.** Access shall be granted under the principle of "less privilege", i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their organizational functions.
- i.** User access review shall be performed at least every three (3) months by the Group or Division that is handling the system or application to determine if the access level given to a user is appropriate and is align with his/her current duties and responsibilities.
- j.** Whenever possible, access should be granted to centrally defined and managed identities.
- k.** Users should refrain from trying to tamper or evade the access control in order to gain greater access than what they are assigned.
- l.** Automatic controls, scan technologies, and periodic revision procedures must be in place to detect any attempt which is made to circumvent controls.

6.3. Password Control Policy.

6.3.1. Purpose. The Password Control Policy section defines the requirements for the proper and secure handling of passwords in the Bureau.

6.3.2. Scope. This policy applies to all officers and employees of the Bureau, including temporary users, visitors, contractors, personnel affiliated with third parties with temporary access to services, and partners with limited or unlimited access time to services.

6.3.3. Policy Definitions.

- a.** Any system that handles valuable information must be protected with a password-based access control system.
- b.** Every user must have a separate and private identity for accessing IT network services.

- c.** Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
- d.** Each identity must have a strong, private, and alphanumeric password to be able to access any service. It should be at least eight (8) characters long, alphanumeric, with special characters (if capable), and more complex than a single word.
- e.** All user-level passwords must be changed at a maximum period of every 90 days, or whenever a system prompts the user to change it. Default passwords must also be changed immediately. If the user becomes aware, or suspects, that his/her password has become known to someone else, the user must change it immediately and report his/her concern to the appropriate MISTG Division.
- f.** Password for some special identities will not expire. In those cases, the password must be at least fifteen (15) characters long.
- g.** Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work-related accounts but also for personal accounts.
- h.** Use of administrative credentials for non-administrative work is discouraged. IT administrators must have two sets of credentials: one for administrative work and one for common work.
- i.** Sharing of passwords is forbidden. Passwords must not be shared with anyone, including supervisors and coworkers. All passwords should be treated with strict confidentiality and should not be revealed or exposed to public sight.
- j.** Never use the "Remember Password" function.
- k.** Never write your passwords down or store them where they are open to theft.
- l.** Do not use the same password on different information systems.

- m. Digital certificates, biometrics, and multiple-factor authentication should be used whenever possible for critical applications.
- n. Identities must be locked if password guessing is suspected on the account.
- o. Application developers must ensure that their programs contain the following security precautions:
 - i. Applications must support the authentication of individual users, not groups.
 - ii. Applications must not store passwords in clear text or any easily reversible form.
 - iii. Applications must not transmit passwords in clear text over the network.
 - iv. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Password Construction Guidelines

- i. **Overview.** Passwords are critical components of information security. They serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or networks. This guideline provides the best practices for creating secure passwords.
- ii. **Purpose.** The purpose of these guidelines shall be to provide the best practices for the creation of strong and secure passwords.
- iii. **Scope.** These guidelines apply to all employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. These guidelines apply to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, and local router logins.

iv. Statement of Guidelines. Strong passwords should be long, i.e., the more characters they contain, the stronger they become. Hence, a password is recommended to have a minimum of fourteen (14) characters. In addition, the use of passphrases, i.e., passwords made up of multiple words, is highly encourage. Examples include "It's time for vacation" or "block-curious-sunny-leaves". Passphrases are both easy to remember and to type, yet meet the strength requirements. Poor, or weak, passwords should have the following characteristics:

1. Contain eight (8) characters or less.
2. Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
3. Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
4. Are some versions of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different and unique password. Whenever possible, it is recommended for the users to enable multi-factor authentications.

6.4. Email Policy. Refer to CMO No. 3-2016² as issued by the Bureau on Email Policy.

6.5. Internet and Network Usage Policy.

6.5.1. Purpose. The Internet Policy section defines the requirements for proper and secure access to the Bureau's internet.

6.5.2. Scope. The Internet Usage Policy applies to all Internet users (individuals working for the Bureau, including officers and employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through computing or networking resources. The Bureau's Internet users are expected to be familiar, and to comply, with this policy and are also required to use their common sense and exercise good judgment while using Internet services.

² CMO No. 3-2016 entitled, "E-Mail Policy for the Bureau of Customs."

6.5.3. Policy Definitions.

- a.** Access to the Internet will be approved and provided only if reasonable organizational needs are identified. Internet services will be granted based on an employee's current job responsibility.
- b.** User Internet access requirements will be reviewed periodically by appropriate Services, Divisions, or Groups to ensure that continuing needs exist.
- c.** Acceptable use of the Internet for performing job functions might include:
 - i.** Communication between employees and non-employees for business purposes.
 - ii.** Technical support downloading software upgrades and patches.
 - iii.** Review of possible vendor websites for product information.
 - iv.** Reference regulatory or technical information.
 - v.** Research.
- d.** The use of Viber service is permitted for organizational purposes.
- e.** Mobile devices (smartphones, tablets, and the likes) are not allowed to connect to the Bureau's network.
- f.** BYOD (bring your own device) will not be allowed to connect to the Bureau's network. Contractors, vendors, and third-party suppliers performing IT-related matters, such as, but not limited to, installation, upgrade, configuration, and maintenance of network devices, servers, and the likes can be allowed to connect to the network with the following provisions:
 - i.** ForeScout Agent will be installed for monitoring and compliance with the following policies:
 - 1.** ForeScout P2P Policy
 - 2.** ForeScout Antivirus Policy
 - 3.** Installed Applications Policy
 - 4.** Device General Information Policy

- ii. FireEye Agent will be installed for protection against cyberattacks, malware, and viruses.
 - iii. Abide all applicable policies within this Information Policy.
- g. Access to pornographic sites, hacking sites, and other risky sites is blocked.
- h. Downloading is a privilege assigned to some users. It can be requested as a service.
- i. Internet access is mainly for business purposes. Limited personal navigation is permitted if in doing so, there is no perceptible consumption of the organization system resources and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
- j. Employees are prohibited from downloading software, other program files, or online services from the Internet, on their assets provided by the Bureau, without prior approval from the MISTG. A request letter should be sent to the Deputy Commissioner, MISTG, for approval.
- k. Downloading, copying, and distributing copyrighted songs, movies, software, and other similar materials are strictly prohibited.
- l. Access to sites and the use of technologies and applications that consume high bandwidth, which may affect the network performance of the Bureau, are strictly prohibited/blocked unless in the performance of responsibilities and duties. High bandwidth consumption may include, but is not limited to:
 - i. Video Streaming Sites (Youtube, Netflix, Spotify, free online video streaming sites, and the likes)
 - ii. File-Sharing Technology (Bit Torrent, Utorrent, Dropbox, and the likes)
- m. Changing the proxy settings to gain access to prohibited sites using VPN (Freemove, Psiphon, Ultrasurf, and the likes) is strictly prohibited.

- n. All sites and downloads may be monitored and/or blocked by MISTG if they are deemed to be harmful and/or not productive to the Bureau. Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back-to-back configuration is strongly recommended for firewalls.
- o. In accessing the Internet, users must behave in a way compatible with the prestige of the Organization. Attacks, like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights, and others, are strictly forbidden.
- p. Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the Information Security Officer.
- q. Reasonable measures must be in place at all servers, workstations, and equipment for the detection and prevention of attacks and abuse. Measures include firewalls, intrusion detection/prevention, and next-generation firewalls.

6.6. Antivirus Policy.

6.6.1. Purpose. The Antivirus Policy section defines the requirements for the proper implementation of anti-virus and other forms of protection in the Bureau.

6.6.2. Scope. This policy applies to all servers, workstations, and equipment in the Bureau, including portable devices, like laptops and mobile devices, that may be brought outside of the agency facilities. Some policies apply to external computers and devices accessing the resources of the Bureau.

6.6.3. Policy Definitions.

- a. Approved anti-virus software must be correctly installed and configured on all supported endpoints and servers across the Bureau's network and domain following the configuration standards. Included also are mobile devices that regularly connect to the Bureau's network.
- b. Anti-virus software must be kept up to date including the definition files.

- c.** Anti-virus software updates must be deployed across the network automatically from the server and it must be configured to check updates.
- d.** Anti-virus software must be configured for real-time scanning and regularly scheduled scans.
- e.** On-access scanning must be configured within Anti-virus software for removable media.
- f.** The anti-virus server must be monitored daily for virus alerts and any issues which cannot be resolved remotely via a centralized management console and must be escalated to the Technical Support Division (TSD) of the MISTG for the deployment of technical support to investigate and resolve the issue.
- g.** The Bureau's computers permanently working in other agencies' networks may be exempted from the previous rule if required by the Security Policies of the other Bureau, provided those computers will be protected too.
- h.** Any server that does not comply with the policy must take steps to mitigate the risk.
- i.** Traveling computers from the agencies that seldom connect to the Bureau's network must have an installed approved antivirus independently managed.
- j.** All the installed anti-virus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
- k.** Visitors' computers and all computers that connect to the Bureau's network are required to stay "healthy", i.e., with a valid and updated antivirus installed.
- l.** Never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- m.** Delete spam, chain, and other junk emails without forwarding them to the Bureau's domain or email.
- n.** Never download files from unknown or suspicious sources.

- o.** Avoid direct disk sharing with reading/write access, unless it is absolutely needed to perform an organization function.
- p.** Always scan flash drives and external hard drives from an unknown source for viruses before using them.
- q.** Back up critical data and system configurations on a regular basis and store the data in a safe place.
- r.** If lab testing or such kind conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the antivirus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus (e.g., email or file sharing).

6.7. Information Classification Policy.

6.7.1. Purpose. The Information Classification Policy section defines a framework for the classification of the information according to its importance and the risks involved. It is aimed at ensuring the appropriate integrity, confidentiality, and availability of the Bureau's information. This policy also helps all officers and employees of the Bureau to ensure that the correct classification and handling methods are applied to their day-to-day responsibilities and duties, and managed them accordingly.

6.7.2. Scope. This policy applies to all the information created, owned, or managed by the Bureau, including those stored in electronic or magnetic forms, and those printed in paper.

6.7.3. Policy Definitions.

- a.** Information Owners shall ensure the security of their information and the systems that support it.
- b.** Information Owners are responsible for ensuring the confidentiality, integrity, and availability of the Bureau's assets, information, data, and IT services.
- c.** Any breach must be reported immediately to the Information Security Officer. If needed, the

appropriate countermeasures must be activated to assess and control damages.

- d. Information in the Bureau is classified according to its security impact. The current categories are **Confidential, Sensitive, Shareable, Public, and Private**.
- e. Information defined as **Confidential** has the highest level of security. Only a limited number of persons must have access to it. Management, access, and responsibilities for confidential information must be handled with special procedures defined by the Information Owners.
- f. Information defined as **Sensitive** must be handled by a greater number of persons. It is needed for the daily performance of jobs and duties, but should not be shared outside of the scope needed in the performance of the related function.
- g. Information defined as **Shareable** can be shared outside of the limits of the Bureau, for clients, organizations, regulators, etc., who acquired or should get access to it.
- h. Information defined as **Public** can be shared as public records (e.g., contents published in the Bureau's public website).
- i. Information deemed as **Private** belongs to individuals who are responsible for their maintenance and backup.
- j. Information is classified **Jointly** by the Information Security Officer and the Information Owner.

6.8. Remote Access Policy.

6.8.1. Purpose. The purpose of this policy is to define rules and requirements for connecting to the Bureau's network from any host outside of its domain. These rules and requirements are designed to minimize the potential exposure of the Bureau from any damages which may result from unauthorized use of the Bureau's resources.

6.8.2. Scope. This policy applies to all users, offices, employees, contractors, vendors, and devices that need

to access the Bureau's internal resources from remote locations.

6.8.3. Policy Definitions.

- a.** To gain access to the internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user, or partner can be requested only by the Information Owner responsible for the information with the assistance of MISTG-TSD and if possible, with the authorization of the Information Security Officer.
- b.** Remote access on desktops units will be allowed provided that prior to connection, the application shall ask permission from the end-user to grant access to his/her device. In line with this, remote access applications such as Team Viewer, Anydesk, and etc. are prohibited.
- c.** Only secure channels with mutual authentication between server and clients shall be available for remote access. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks) and strong passphrases. Both server and clients must receive mutually trusted certificates.
- d.** Authorized User shall protect their login and password with strict confidentiality.
- e.** Remote access to confidential information should not be allowed. An exception to this rule may only be authorized by the Information Owner in cases where it is strictly needed.
- f.** All hosts that are connected to the Bureau's internal networks and information systems via remote access technologies must use the most up-to-date anti-virus software.
- g.** Users must not connect to the Bureau's network from public computers unless the access is for viewing public content.

6.9. Software and Hardware Installation Policy.

6.9.1. Purpose. The purpose of this policy is to outline the requirements for installing software and hardware on the

Bureau's computing devices to minimize the risk of loss of program functionality, the exposure of sensitive information contained within the Bureau's computing network, the risk of introducing malware, the introduction of malware from infected installation software, and legal exposure of running unlicensed software (which could be discovered during IT Audit).

6.9.2. Scope. This policy applies to all officers, employees, contractors, and vendors. It also covers all computers, servers, smartphones, tablets, and other computing devices used within the Bureau; all software or applications, whether purchased, leased, obtained under 'shareware' or 'freeware' arrangements, and developed in-house.

6.9.3. Policy Definitions.

a. Employees may not install software and applications on Bureau's computing devices operated within the Bureau's network.

b. Authorized software and applications:

i. Productivity Tools

- 1.** Microsoft Office 2013 and latest versions
- 2.** Microsoft Office 365
- 3.** Java
- 4.** Acrobat Reader DC
- 5.** 7 Zip

ii. Web Browser

- 1.** Internet Explorer
- 2.** Microsoft Edge
- 3.** Google Chrome
- 4.** By default, browser extensions are disabled

iii. Security and Monitoring

- 1.** ForeScout
- 2.** FireEye
- 3.** McAfee Antivirus
- 4.** McAfee DLP Endpoint (browser extension)

c. Software requests must first be approved by the requester's immediate supervisor. The, the same shall be submitted to the MISTG using the Policy Exemption Form (see Annex B).

- d. Software and application upgrades and patching must only be done by the MISTG- TSD.
- e. The MISTG-TSD will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.
- f. Software or application copied from one computer to another, or copies made of software media or manuals, without the explicit confirmation from the MISTG-TSD that this is in accordance with the appropriate licensing agreement, contract, service level agreement, and with copyright law, are prohibited.
- g. Normally, only the current version of a software/application and its immediate predecessor will be implemented and supported. In some cases, technical, support, or licensing issues may preclude the use of a much older version of the software.
- h. Contractors, suppliers, consultants, and temporary staff are covered by the terms of this policy and must not introduce unlicensed or inappropriate software to the Bureau's computers, networks and domain.
- i. Installation and configuration of hardware peripherals such as scanners, printers, web cameras, memory card readers, and etc., must be done by MISTG-TSD.
- j. Upgrades on the current system units such as an increase in memory, upgraded processor, and installation of video cards must be done only in the performance of highly technical jobs that needs an increase of computing resources with the written approval of the immediate supervisor. Installation and configuration of the upgrade components must be done only by the MISTG-TSD.

6.10. Desktop Support Policy.

6.10.1. Purpose. The purpose of this policy is to have desktop support guidelines for hardware, software, and peripherals owned by the Bureau and used by its officers and employees.

6.10.2. Scope. This policy covers all computers, printers, network devices, and software owned or leased by the Bureau.

6.10.3. Policy Definitions.

- a. Full support for computers, printers, network devices, and software include the following:
 - i. Initial installation and setup
 - ii. Diagnosis, recommendation, and correction of reported problems.
 - iii. Upgrades (as needed)

Request for hardware upgrades will be evaluated to determine if they are appropriate and recommendations will be made by Systems Management Division (SMD) of the MISTG.

- b. If a computer will be out for repair for longer than one (1) day, a temporary replacement will be provided that can be used to perform daily tasks and duties.
- c. Requests will be prioritized according to the urgency and number of users affected.
 - i. Problems affecting an entire department (i.e. network switch problem or a network printer problem) will usually take priority over individual problems.
 - ii. Computers that are affected by malware and viruses are given high priority because of their destructive potential and ability to infect other computers.
 - iii. Non-operational computers will receive a higher priority than machines that are experiencing non-critical or intermittent problems.
- d. MISTG-SMD will utilize remote connection applications, whenever appropriate, to provide quick resolution (the user's permission is required for remote connection access).

- e. Defective units which have hardware-related problems that are still under warranty will be sent to the supplier for warranty purposes.
- f. In the event that a computer must be reimaged, reformatted, and other similar procedures, MISTG-SMD will not be responsible for the backup and restoration of data files.
- g. The Bureau's employees should be familiar with basic printer operations (i.e., how to power the printer up/down, how to clear a paper jam, printer physical connection to computer). MISTG-SMD will provide first-level support to printers (i.e., installation, configuration, changing of ink cartridge). Hardware-related problems should be sent to an authorized service center by the group or division owner.

6.11. Removable Media Policy.

6.11.1. Purpose. The purpose of this policy is to minimize the risk of damage computing devices, loss or exposure of sensitive information owned and maintained by the Bureau, and to reduce the risk on removable media of acquiring malware infections on computing devices operated by the Bureau.

6.11.2. Scope. This policy covers all computers and servers operating in the Bureau.

6.11.3. Removable Media and Devices.

- a. Optical Discs (Blu-ray discs, DVDs, CD-ROMs)
- b. Memory Cards (Compact Flash card, Secure Digital card, Memory Stick)
- c. USB flash drives
- d. External hard drives (IDE, EIDE, SCSI, and SSD)
- e. Digital cameras
- f. Smartphones
- g. Other external/dockable devices which contain removable media capabilities

6.11.4. Policy Definitions.

- a. Sensitive information may be stored on removable media only when required in the performance of assigned duties or when providing information required by other government agencies.

- b.** There must be an installed anti-virus solution on every computer that will actively scan for malware when any type of removable media or device is connected.
- c.** If capable, ensure that all removable media and devices are encrypted. This will render any data useless to unauthorized users should the device be lost or stolen.
- d.** Never connect found media or devices to a personal computer (PC). Give any unknown storage device to the security or IT personnel.
- e.** Never disclose the passwords used with removable media or devices to anyone.
- f.** Disable the Autorun and Auto-play features for all removable media or devices. These features automatically run when plugged into a USB port or drive.
- g.** Keep your personal and organizational data in separate devices.
- h.** When you have finished transferring sensitive data from removable media or device, be sure to delete it from that device.
- i.** Formal procedures for the secure disposal of media should be established to minimize risks. The following controls should be considered:
 - i.** Media containing sensitive information should be stored and disposed of securely and safely (e.g. by incineration or shredding or emptied of information for use by another application within the organization).
 - ii.** Some CDs and DVDs can only be written on once; others may be rewritable. In either case, in order to be sure that the data is adequately protected, the best method for disposal of these disks is to physically destroy them. Breaking the disks into pieces and disposing of them as normal wastes is suitable for non-sensitive data.

- iii. Disposal of sensitive items should be logged, if possible, in order to maintain an audit trail.
- iv. If hard disk drives will be reused for other purposes, overwrite media using industry-standard overwriting technologies/methods/tools.

6.12. Clean Desk Policy.

6.12.1. Purpose. The purpose of this policy is to establish the minimum requirements for maintaining a “clean desk” – where sensitive/critical IT-related or computer-generated information about the Bureau’s employees, customs’ processes, clients, and third parties are secured in locked areas and out of sight. A Clean Desk policy is not only compliant to the International Organization for Standardization (ISO) 27001/17799, but it is also part of the standard basic privacy controls.

6.12.2. Scope. This policy applies to all officers and employees of the Bureau.

6.12.3. Policy Definitions.

- a. Employees are required to ensure that all sensitive/confidential information in hard copies or electronic forms are secured in their work area at the end of the day and when they are expected to be gone for an extended period.
- b. Computer workstations must be locked when the workspace is unoccupied.
- c. Computer workstations must be shut completely down at the end of the workday.
- d. Any Restricted or Sensitive information must be removed from the desk or locked in a drawer whenever the desk is unoccupied and at the end of the workday.
- e. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- f. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

- g.** Laptops must be either locked with a locking cable or locked away in a drawer.
- h.** Passwords may not be left on sticky notes posted on, or under, a computer, nor may they be left written down in an accessible location.
- i.** Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- j.** Upon disposal, Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins.
- k.** Whiteboards containing Restricted and/or Sensitive information should be erased.
- l.** Lock away portable computing devices such as laptops and tablets.
- m.** Treat mass storage devices, such as CDROM, DVD, or USB drives, with strict confidentiality and secure them in a locked drawer.
- n.** All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays to prevent any wrongful or unauthorized person to pick them up.

6.13. Workstation Security Policy.

6.13.1. Purpose. The purpose of this policy is to provide guidance on the security for the Bureau's workstations to ensure the security of the information contained therein, and the information it may have access to.

6.13.2. Scope. This policy applies to all officers, employees, contractors, and vendors with a Bureau-owned or personal workstation connected to the network and domain of the Bureau.

6.13.3. Policy Definition. Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity, and availability of sensitive information and that access to sensitive information is restricted to authorized users.

- a.** Workforce members using workstations shall consider the sensitivity of the information that may be accessed, to minimize the possibility of unauthorized access thereon.
- b.** The Bureau will implement physical and technical safeguards for all workstations that access electronically-protected health information to restrict access to authorized users.

Appropriate measures include:

- i.** Restricting physical access to workstations to only authorized personnel.
- ii.** Securing workstations (screen lock or logout) prior to leaving the area to prevent unauthorized access.
- iii.** Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with the Bureau's Password Policy.
- iv.** Complying with all applicable password policies and procedures. See Bureau of Customs' Password Policy.
- v.** Ensuring workstations are used for authorized organizational purposes only.
- vi.** Never install unauthorized software on workstations.
- vii.** Keeping food and drink away from workstations in order to avoid accidental spills.
- viii.** Securing laptops that contain sensitive information by using cable locks, or locking it away in drawers or cabinets.
- ix.** Installing privacy screen filters or using other physical barriers to alleviate exposure data.
- x.** Ensuring workstations while left on, are logged off, in order to facilitate after-hours updates.

xi. Exit running applications and close open documents.

xii. Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).

6.14. Virtual Private Network (VPN) Policy.

6.14.1. Purpose. The purpose of this policy is to provide guidelines for Remote Access IPsec or L2TP VPN connections to the Bureau's network.

6.14.2. Scope. This policy applies to all officers, employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties utilizing VPNs to access the Bureau's network. This policy applies to implementations of VPN that are directed through an IPsec Concentrator.

6.14.3. Policy Definitions. Only approved Bureau employees may use VPNs for connection to its network. VPN ID Request Form (**Annex D**) must be accomplished by the immediate supervisor of the personnel to be given VPN access. VPN client software will be issued to approve users by the MISTG-TSD. The user is responsible for arranging an Internet Service Provider (ISP) connection and paying associated fees. Further, details may be found in the **Remote Access Policy**.

a. Additionally:

i. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to the Bureau's networks.

ii. 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.

iii. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

iv. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

- v. All computers connected to the Bureau's network via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.
- vi. Users must ensure that their computers have the most up-to-date security patches applied.
- vii. VPN users will be automatically disconnected from the Bureau's network after thirty (30) minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- viii. The VPN concentrator is limited to an absolute connection time of 24 hours.
- ix. Users of computers that are not Bureau-owned equipment must configure the equipment to comply with Bureau's VPN and other associated policies.
- x. 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 Bureau-owned equipment (i.e., their machines must be configured to comply with Infosec's Security Policies).
- xi. Network connection activity may be logged and monitored for security purposes.

6.15. Outsourcing Policy.

6.15.1. Purpose. The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions, and processes.

6.15.2. Scope. This policy applies to the Bureau, its services providers to whom IT services, functions, or processes are outsourced, and the outsourcing process itself.

6.15.3. Policy Definitions.

- a.** Before outsourcing any service, function, or process, a careful strategy must be followed to evaluate the risks and financial implications and a Non-Disclosure Agreement (NDA) needs to be signed.
- b.** Whenever possible, a bidding process should be followed to select between several service providers.
- c.** In any case, criteria for selecting an outsourcer or service provider shall be defined considering the following:
 - i.** Company's reputation and history
 - ii.** Quality of services provided to other customers (private and government)
 - iii.** Number and competence of staff and managers
 - iv.** Financial stability of the company and commercial record
 - v.** Retention rates of the company's employees
 - vi.** Quality assurance and security management standards are currently followed by the company (i.e., ISO 9000 and ISO/IEC 27001).
- d.** Audits should be planned to evaluate the performance of the service provider before and during the provision of the outsourced service, function, or process.
- e.** A service contract and defined service levels must be agreed upon between the Bureau and the service provider.
- f.** If the information being exchanged or processed is sensitive or confidential in nature, a binding confidentiality agreement shall be in place between the Bureau and the outsourcer. A separate NDA is required.
- g.** Information shall be classified and controlled accordingly with the Bureau's policies.
- h.** The service provider must get authorization from the Bureau if it intends to hire a third party to support the outsourced service, function, or process.

- i. The service provider shall implement appropriate security measures and comply with the Data Privacy Act, its implementing rules and regulations, and other issuances of the National Privacy Commission.
- j. The service provider shall assist the personal information controller of the Bureau, by appropriate technical and organizational measures, and to the extent possible, fulfill the obligation to respond to requests by the information owners relative to the exercise of their rights.
- k. The service provider shall assist the personal information controller of the Bureau in ensuring compliance with the Data Privacy Act, its implementing rules and regulations, other relevant laws, and other issuances of the National Privacy Commission, taking into account the nature of processing and the information available to the personal information processor.
- l. The service provider shall delete or return all personal data to the Bureau's personal information controller after the end of the provision of services relating to the processing, including deleting existing copies, unless storage is authorized by the Data Privacy Act or other laws.
- m. The service provider shall make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Data Privacy Act, and allow for, and contribute to, audits, including inspections conducted by the personal information controller or another auditor mandated by the Bureau.
- n. The service provider shall immediately inform the personal information controller of the Bureau if, in its opinion, an instruction infringes the Data Privacy Act, its implementing rules and regulation, or any other issuances of the National Privacy Commission.

6.15.4. Service Level Agreement (SLA). SLA between the Bureau and service providers should fall in these service levels:

- a. **Customer-based SLA:** An agreement with an individual customer group, covering all the services they use. For example, an SLA between a supplier (IT service provider) and the Accounting Division for the services, such as finance system, payroll system, billing system, procurement/purchase system, and etc.
- b. **Service-based SLA:** An agreement for all customers using the services being delivered by the service provider. For example, an email system for the entire organization.
- c. **Multi-level SLA:** This agreement is customized according to the needs of the end-user company. It allows the user to integrate several conditions into the same system to create a more suitable service. It addresses contracts at the following levels:
 - i. **Corporate level:** This SLA does not require frequent updates since its issues are typically unchanging. It includes a comprehensive discussion of all the relevant aspects of the agreement and applies to all customers in the end-user organization.
 - ii. **Customer level:** This contract discusses all service issues that are associated with a specific group of customers. However, it does not take into consideration the type of user services. An example of this is when an organization requests that the security level in one of its departments is strengthened. In this situation, the entire company is secured by one security agency but requires that one of its customers in the company is more secure for certain reasons.
 - iii. **Service level:** In this agreement, all aspects that are attributed to a particular service regarding a customer group are included.

d. Components.

- i. **Type of service to be provided:** It specifies the type of service and any additional details of the type of service to be provided. In the case of an IP network connectivity, the type of service will describe functions such as operation and

maintenance of networking equipment, connection bandwidth to be provided, and etc.

- ii.** The service's desired performance level, specially its reliability and responsiveness: A reliable service will be the one that suffers minimum disruptions in a specific amount of time and is available at almost all times. Service with good responsiveness will perform the desired action promptly after the customer requests it.
- iii.** Monitoring process and service level reporting: This component describes how the performance levels are supervised and monitored. This process involves gathering different types of statistics, how frequently these statistics will be collected, and how these statistics will be accessed by the customers.
- iv.** The steps for reporting issues with the service: This component will specify the contact details to report a problem and the order in which details about the issue have to be reported. The contract will also include a time range in which the problem will be appropriately acted upon and also until when the issue will be resolved.
- v.** Response and issue resolution timeframe: The response time frame is the period by which the service provider will start the investigation of the issue. Issue resolution timeframe is the period by which the current service issue will be resolved and fixed.
- vi.** Repercussions for the service provider not meeting its commitment: If the provider is not able to meet the requirements as stated in SLA then the service provider will be subjected to consequences. These consequences may include the customer's right to terminate the contract and refund for losses incurred by the customer due to failure of service.
- vii.** The service provider and their employees shall, if the processing includes personal data, register their personal data processing system with the National Privacy Commission in accordance with

the Data Privacy Act and its implementing rules and regulations.

6.16. Data Protection and Privacy of Personal Information Policy.

6.16.1. Purpose. The Data Protection and Privacy of Personal Information Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions, and processes.

6.16.2. Scope. This policy applies to the Bureau, its services providers to whom IT services, functions, or processes are outsourced, and the outsourcing process itself. Issuances related to data protection and privacy of personal information, such as CMO No. 16-2021³ shall be complementary with this Order.

6.16.3. Policy Definitions.

- a.** All users must not bring personal effects to the Bureau's premises or use the Bureau's systems for private communications without understanding that these may be searched or randomly monitored.
- b.** The Bureau must not, at any time, gather personal information using misrepresentations or pretext statements about its right to receive such information.
- c.** The Bureau must retain the right to release private and confidential information to outside parties in order to collect outstanding bills or to otherwise compel performance with contractual terms and conditions.
- d.** Private information records must be disclosed only to a person who is actively engaged in a professional relationship with the individual or when the individual provides written authorization.
- e.** Before any service is provided, clients and users must provide written consent⁴ (please see Annex C) for the disclosure of their private information to the Bureau's officials, and authorized third parties, who need such

³ CMO No. 16-2021 entitled, "Privacy Manual".

⁴ CMO No. 16-2021, Section 11.7.

- access in order to perform the requested services, unless the local office head has waived this requirement.
- f.** The Bureau must collect, process, store, and disseminate information only that is necessary for the proper performance of its function.
 - g.** The Bureau's workers and information systems must not collect private information, unless this effort has been approved in advance by the Bureau's legal service.
 - h.** Before the Bureau's workers collect private information about workers, clients, or other people, the need for such information must be documented and approved by the Human Resources Management.
 - i.** The collection of private data by the Bureau's workers must be performed by lawful means, and only for purposes related to the activities of the Bureau.
 - j.** The Bureau's computer and communications systems must not collect private data from clients or potential clients without having obtained their clear and unambiguous consent.
 - k.** The Bureau must provide its clients and prospects with full and accurate descriptions of all private data captured as well as everything that is done with that data, whenever the client wishes to exercise his right to be informed as part of his data privacy rights.
 - l.** The Bureau must obtain written consent (please see Annex C) from customers before it records any information about them in a computerized information system.
 - m.** All individuals must be offered a notice about the Bureau's privacy practices and must be given sufficient time to read and ask questions about these before they provide written consent (Annex C) that permits the use of their private data.
 - n.** In every instance where personal identifiable information is collected, an explicit and understandable notice (please see Annex C) must be provided at the time and place the information is collected.

- o.** The Bureau must not place invisible software or invisible information on the machine of any user who has visited either the Bureau’s web or any other Bureau-affiliated site and must not in any way covertly change the software or information resident on the machine of these users.
- p.** The Data Privacy Policy of the Bureau (Annex E) must be posted in its Official Website or any of its online systems where personal information is collected or processed.
- q.** Every user who will access the Official Website or any online systems of the Bureau must be informed of the Data Privacy Policy through a pop-up notice or any other means, as may be applicable, where continuous access of the said website or system is an implied agreement to the said policy.

Section 7. Policy Compliance.

7.1. Compliance Measurement. The MISTG shall verify compliance to these policies through various methods, including but not limited to:

7.1.1. Monitoring Tools. MISTG shall use Network Access Control, Network Monitoring Tool, Desktop Management Solution, Next-Generation Firewall, and the likes for daily monitoring and implementation of system-related policies.

7.1.2. Periodic Reviews. Periodic assessments of Access Level, VPN Access, Remote Access, and Policy Exemption to determine whether these privileges are aligned with the current duties and responsibilities of the user.

7.1.3. IT Audit. MISTG-SMD and Information Security Officers shall perform an IT Audit, at least once a year, to Bureau of Custom’s Head office, ports and sub-ports. The IT audit team shall examine and evaluate the IT infrastructure, applications, and procedures to validate compliance to the Information Security Policy.

7.1.4. Report. Heads of Groups and Divisions are encouraged to report any suspected violations or concerns of personnel under their management as to the compliance with the Information Security Policy.

- 7.2. Exemptions.** Request for exemption from any of these policies must be applied by submitting a fully accomplished Policy Exemption Form (see Annex B). The maximum period of the policy exemption shall be one (1) year. All exemptions shall automatically be revoked and terminated on the first working day after the exemptions have expired. For renewal, a new application for exemption shall be filed and shall be subject to the approval of the Chief Information Officer.
- 7.3. Non-Compliance.** Any employee found to have violated this policy shall be subject to the following administrative penalties:

1st Offense: Reprimand;
2nd Offense: Suspension of one (1) to thirty (30) days;
and
3rd Offense: Dismissal from the Service.

The penalties provided for in this manual shall be without prejudice to other criminal, administrative, or civil liability that may arise pursuant to the provisions of the law violated.

The Revised Rules on Administrative Cases in the Civil Service shall be applicable in the disposition of cases under this manual.

Section 8. Revision of Policies. The Bureau, upon recommendation of the MISTG, may replace, modify, revise, add, or remove terms and provisions of the policies herein provided, as allowed by applicable laws, to conform to current situation and change of environment.

Section 9. Repealing Clause. All other Orders, Memoranda, Circular or parts thereof which are inconsistent with this CMO are hereby deemed repealed and/or modified accordingly.

Section 10. Effectivity. This Order shall take effect five (5) days after its publication in a newspaper of general circulation.

The Office of National Administrative Register of the UP Law Center shall be provided three (3) certified copies of this Order.


REY LEONARDO B. GUERRERO
Commissioner *ag*
 BOC-02-07684

REVISION HISTORY

Date of Change	Responsible	Summary of Change

GLOSSARY

Term	Definition
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Availability	Data or information is accessible and usable upon demand by an authorized person.
Confidentiality	Data or information is not made available or disclosed to unauthorized persons or processes.
Identity	A unique name that is used to identify a user, person, or role.
Integrity	Data or information has not been altered or destroyed in an unauthorized manner.
Identity	A unique name that is used to identify a user, person, or role.
Information Security Policy	The policy that governs the Bureau's approach to information security management
ISO 9001	Is defined as the international standard that specifies requirements for a quality management system (QMS). Organizations use the standard to demonstrate the ability to consistently provide products and services that meet customer and regulatory requirements. It is the most popular standard in the ISO 9000 series and the only standard in the series to which organizations can certify.
ISO 27001	Specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure, etc.
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. The probability of a loss of confidentiality, integrity, or availability of information resources.
Service Level Agreement	Defines the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties.

Topic Index

INTRODUCTION	1
SECTION 1. OBJECTIVES	1
SECTION 2. SCOPE	2
SECTION 3. PERSONNEL SECURITY	2
SECTION 4. GENERAL POLICY	3
SECTION 5. EXCEPTIONS TO POLICIES	3
SECTION 6. POLICIES	3
6.1. IT Assets Acceptable Use Policy	3
6.1.1. Purpose	3
6.1.2. Scope.....	3
6.1.3. Policy Definitions.....	4
6.2. Access Control Policy	9
6.2.1. Purpose	9
6.2.2. Scope	9
6.2.3. Policy Definitions	10
6.3. Password Control Policy	11
6.3.1. Purpose	11
6.3.2. Scope	11
6.3.3. Policy Definitions	11
6.4. Email Policy	14
6.5. Internet and Network Usage Policy	14
6.5.1. Purpose	14
6.5.2. Scope.....	14
6.5.3. Policy Definitions.....	15
6.6. Antivirus Policy	17
6.6.1. Purpose	17
6.6.2. Scope.....	17
6.6.3. Policy Definitions.....	17
6.7. Information Classification Policy	19
6.7.1. Purpose	19
6.7.2. Scope.....	19
6.7.3. Policy Definitions.....	19
6.8. Remote Access Policy	20
6.8.1. Purpose	20
6.8.2. Scope	20
6.8.3. Policy Definitions.....	21
6.9. Software and Hardware Installation Policy	21
6.9.1. Purpose	21
6.9.2. Scope.....	22
6.9.3. Policy Definitions.....	22
6.10. Desktop Support Policy	23
6.10.1. Purpose.....	23
6.10.2. Scope	24
6.10.3. Policy Definitions	24
6.11. Removable Media Policy	25
6.11.1. Purpose.....	25
6.11.2. Scope	25
6.11.3. Removable Media and Devices.....	25
6.11.4. Policy Definitions	25
6.12. Clean Desk Policy	27
6.12.1. Purpose.....	27
6.12.2. Scope	27
6.12.3. Policy Definitions	27

6.13. Workstation Security Policy	28
6.13.1. Purpose.....	28
6.13.2. Scope.....	28
6.13.3. Policy Definition	28
6.14. Virtual Private Network (VPN) Policy.....	30
6.14.1. Purpose.....	30
6.14.2. Scope.....	30
6.14.3. Policy Definitions	30
6.15. Outsourcing Policy	31
6.15.1. Purpose.....	31
6.15.2. Scope.....	31
6.15.3. Policy Definitions	32
6.15.4. Service Level Agreement (SLA)	33
6.16. Data Protection and Privacy of Personal Information Policy.	36
6.13.1. Purpose.....	36
6.13.2. Scope.....	36
6.16.3. Policy Definitions	36
SECTION 7. POLICY COMPLIANCE	38
SECTION 8. REVISION OF POLICIES	39
SECTION 9. EFFECTIVITY	39



Republic of the Philippines
 Department of Finance
BUREAU OF CUSTOMS

POLICY EXEMPTION FORM

Requester Name: _____ Date of Request: _____
 Requestor Office: _____

Policy Name and Section	Exemption Duration	Justification (describe in detail)

******All policy exemptions must be renewed every first working day after the policy exemption has expired ******

 Signature

INDORSED BY:

APPROVED/DISAPPROVED
Unit Head
DATE:

INDORSED BY:

APPROVED/DISAPPROVED
Information Security Officer
DATE:

INDORSED BY

APPROVED/DISAPPROVED
Chief TSD/SMD, MISTG
DATE:

APPROVED BY:

APPROVED/DISAPPROVED
Deputy Commissioner, MISTG
DATE:



Republic of the Philippines
Department of Finance
BUREAU OF CUSTOMS

PRIVACY NOTICE AND CONSENT FORM

I. Consent

I, _____
(Full Name)
of

(Residential Address)

hereby state that I have read and understood the attached information. I hereby authorize the employees and independent contractors of the Bureau of Customs, including their directors, officers, and employees, to obtain relevant information from, and release relevant information to, the parties described on page 2 of this form to assist with my involvement with the Bureau. I understand that I can revoke my authority at any time. I acknowledge that if I revoke my authority, or if I decline to provide information as requested by the Bureau, the latter may be unable to provide the services I have requested.

Signed: _____

Date (mm/dd/yy): _____

II. Privacy

The **BUREAU OF CUSTOMS** is committed to protecting and respecting your privacy in compliance with the Data Privacy Act (Republic Act No. 10173). We want to tell you how we use and protect your personal information. This includes informing you of your rights regarding your personal information that we hold. The Bureau also has a full privacy policy which can be found on our website www.customs.gov.ph.

III. Information, Collection, Use, and Disclosure

During the course of your involvement with the Bureau of Customs, we may collect, use or disclose personal information about you for the following purposes:

- Assisting you in your Import Transactions;
- Assisting you in your Export Transactions;
- Assisting you in your Airport Operations;
- Assisting you in processing of Tax Exemption Certificates;
- Assisting you in issuance of Clearance of No Pending Case by the Legal Service;

- Assisting you in issuance of Clearance of No Pending Case by the CIIS;
- Assisting you in processing of application for Drawback (One Stop Shop Drawback Center);
- Assisting you in processing of the request for the utilization of BOC approved TCC;
- Assisting you in processing of the request for the utilization of TCC jointly issued by BOC-OSS;
- Assisting you in processing of application for special revalidation of TCC with the Tax Credit Committee;
- Assisting you in processing of application for special revalidation of TCC District Collector's Office (Reduction of Duty Rate);
- Assisting you in processing of application for VAT Refund through Tax Credit;
- Assisting you in processing of application for employment or job contracting with the Bureau;
- Use of the Information and Communications System of the Bureau;
- Assisting you in processing of data requests with the Bureau;
- Assisting you in entering into agreements with the Bureau;
- Recording or accessing information on the E2M and other online system of the Bureau;

The types of personal information we may collect, use or disclose about you includes but is not limited to:

- Your full name;
- Your date of birth;
- Your residential address;
- Your postal address;
- Your email address;
- Your home telephone number;
- Your work telephone number;
- Your mobile telephone number;
- Your occupation and business address;
- Financial information including details of your employer, income, name of bank or financial institution;
- Details of your spouse, de facto, and dependent children.
- Details of properties owned by you.

In order to provide services to you, we may disclose your personal information to the persons/organizations described below:

- Your legal advisor(s) and the legal advisor(s) representing the other party(s) involved in your transaction;
- Your financial institution and/or financial advisor;
- Insurance providers and brokers;
- Utility providers and utility connection service providers;
- Persons or organizations involved in providing, managing or administering your shipment or goods including independent contractors engaged by the Bureau.

- Tradespeople engaged by us to repair or maintain a property owned or leased by you;
- Organizations involved in maintaining, reviewing and developing the Bureau's systems, procedures and infrastructure including maintaining or upgrading our computer systems;
- Organizations involved in the payments systems including financial institutions, merchants, and payment organizations;
- Tariff Commission;
- Bureau of Internal Revenue;
- Department of Finance;
- Philippine National Police;
- National Bureau of Investigation;
- Other Government Agencies;
- With third parties because you have given consent.

Whenever it is reasonable or practicable to do so, we will collect your personal information directly from you. Sometimes it will be necessary for us to collect information from a third party or a publicly available source, such as your legal adviser, your past or current employers, your past or current clients, and your past or current brokers or agents.

In the course of providing services to you, it may be necessary for us to enter your personal information into forms generation software and customs websites. Depending on the terms of use of such software and websites, a third party may acquire rights to use or disclose information entered into the relevant forms or websites.

We need your permission to collect, use, and disclose your personal information and we therefore ask that you sign the consent on the first page of this document to indicate your consent.

In the event that you do not consent to the Bureau of Customs collecting and releasing your personal information as described above, we may be unable to provide the services requested by you.

IV. Access to, and correction of personal information

You have the right to request access to your personal information and to request that the Bureau update or correct your personal information.

Our privacy policy contains further information about how you may request access to, and correction of, your personal information.

V. Contacting Us

You may contact us by mail, email or telephone as follows:

Mail:



Public Information and Assistance Division (PIAD) Office located at the Office of the Commissioner Building, Gate 3, South Harbor, Port Area, Manila

E-mail:

piad@customs.gov.ph

Telephone:

8705-6000

 <small>Dep. 2015-0715</small>		BUREAU OF CUSTOMS e-Customs Project VPN ID REQUEST FORM	REQUEST NO: _____ Received by _____ Date & Time _____																
<table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> POM</td> <td><input type="checkbox"/> BATANGAS</td> <td><input type="checkbox"/> ZAMBOANGA</td> <td><input type="checkbox"/> SAN FERNANDO</td> </tr> <tr> <td><input type="checkbox"/> MICP</td> <td><input type="checkbox"/> SUBIC</td> <td><input type="checkbox"/> ILOILO</td> <td><input type="checkbox"/> TACLOBAN</td> </tr> <tr> <td><input type="checkbox"/> NAIA</td> <td><input type="checkbox"/> CLARK</td> <td><input type="checkbox"/> SURIGAO</td> <td><input type="checkbox"/> DAVAO</td> </tr> <tr> <td><input type="checkbox"/> CEBU</td> <td><input type="checkbox"/> CAGAYAN</td> <td><input type="checkbox"/> LEGASPI</td> <td><input type="checkbox"/> OTHERS, specify _____</td> </tr> </table>				<input type="checkbox"/> POM	<input type="checkbox"/> BATANGAS	<input type="checkbox"/> ZAMBOANGA	<input type="checkbox"/> SAN FERNANDO	<input type="checkbox"/> MICP	<input type="checkbox"/> SUBIC	<input type="checkbox"/> ILOILO	<input type="checkbox"/> TACLOBAN	<input type="checkbox"/> NAIA	<input type="checkbox"/> CLARK	<input type="checkbox"/> SURIGAO	<input type="checkbox"/> DAVAO	<input type="checkbox"/> CEBU	<input type="checkbox"/> CAGAYAN	<input type="checkbox"/> LEGASPI	<input type="checkbox"/> OTHERS, specify _____
<input type="checkbox"/> POM	<input type="checkbox"/> BATANGAS	<input type="checkbox"/> ZAMBOANGA	<input type="checkbox"/> SAN FERNANDO																
<input type="checkbox"/> MICP	<input type="checkbox"/> SUBIC	<input type="checkbox"/> ILOILO	<input type="checkbox"/> TACLOBAN																
<input type="checkbox"/> NAIA	<input type="checkbox"/> CLARK	<input type="checkbox"/> SURIGAO	<input type="checkbox"/> DAVAO																
<input type="checkbox"/> CEBU	<input type="checkbox"/> CAGAYAN	<input type="checkbox"/> LEGASPI	<input type="checkbox"/> OTHERS, specify _____																
LOGIN REQUEST FOR: (Name of system user to be given access) Name _____ Signature _____ Position/Designation _____ Office/Agency _____ Tel. No. _____ Email _____ PC/Laptop MAC Address: _____																			
*ATTACHED DOCUMENTS (Certified true copy of documents required for submission) <input type="checkbox"/> CPO designating the BOC Personnel to the position requiring e-Customs Access <input type="checkbox"/> Certificate of Assumption of Duty <input type="checkbox"/> Certificate/s of Training (e-Customs) <input type="checkbox"/> Indorsement from the District/Port Collector or DepComm where the personnel is assigned <input type="checkbox"/> For IG & EG Personnel -- Clearance from DepComm, IG or EG <input type="checkbox"/> For OCOM Personnel -- Clearance from the Commissioner or Chief-of-Staff <i>*for BOC Personnel ONLY</i>																			
Reason/s for Request and Time: _____ _____																			
Requested by (Should be filled out by the immediate superior of the personnel to be given access) Name _____ Signature _____ Position/Designation _____ Office/Agency _____																			
FOR MISTG USE ONLY Special Instruction: Recommend Approval/Disapproval: _____ <div style="text-align: center;"> JONATHAN T. SORIANO OIC-Director, TMS-MISTG </div> <div style="text-align: right;"> _____ Date/Time </div>																			
APPROVED/DISAPPROVED: _____ <div style="text-align: center;"> ALLAN C. GERONIMO Deputy Commissioner, MISTG </div> <div style="text-align: right;"> _____ Date/Time </div>																			
ACTION TAKEN <input type="checkbox"/> Creation <input type="checkbox"/> Modification <input type="checkbox"/> Reactivation <input type="checkbox"/> Deactivation <input type="checkbox"/> Others by: _____ <div style="text-align: center;"> VPN/ Network Admin </div> <div style="text-align: right;"> _____ Date/Time </div>																			
LOGIN NAME _____																			
When applicable, this portion to be given back to the requesting BOC/Other Agency personnel NAME OF USER: _____ LOGIN NAME: _____ INITIAL PASSWORD: _____																			

DATA PRIVACY POLICY OF THE BUREAU OF CUSTOMS

The **BUREAU OF CUSTOMS** is committed to protecting and respecting your privacy in compliance with the Data Privacy Act (Republic Act No. 10173). We want to tell you how we use and protect your personal information. This includes informing you of your rights regarding your personal information that we hold. The Bureau also has a full privacy policy which can be found on our website www.customs.gov.ph.

I. Information, Collection, Use, and Disclosure

During the course of your involvement with the Bureau of Customs, we may collect, use or disclose personal information about you for the following purposes:

- Assisting you in your Import Transactions;
- Assisting you in your Export Transactions;
- Assisting you in your Airport Operations;
- Assisting you in processing of Tax Exemption Certificates;
- Assisting you in issuance of Clearance of No Pending Case by the Legal Service;
- Assisting you in issuance of Clearance of No Pending Case by the CIIS;
- Assisting you in processing of application for Drawback (One Stop Shop Drawback Center);
- Assisting you in processing of the request for the utilization of BOC approved TCC;
- Assisting you in processing of the request for the utilization of TCC jointly issued by BOC-OSS;
- Assisting you in processing of application for special revalidation of TCC with the Tax Credit Committee;
- Assisting you in processing of application for special revalidation of TCC District Collector's Office (Reduction of Duty Rate);
- Assisting you in processing of application for VAT Refund through Tax Credit;
- Assisting you in processing of application for employment or job contracting with the Bureau;
- Use of the Information and Communications System of the Bureau;
- Assisting you in processing of data requests with the Bureau;
- Assisting you in entering into agreements with the Bureau;
- Recording or accessing information on the E2M and other online system of the Bureau;

The types of personal information we may collect, use or disclose about you includes but is not limited to:

- Your full name;
- Your date of birth;
- Your residential address;
- Your postal address;
- Your email address;

- Your home telephone number;
- Your work telephone number;
- Your mobile telephone number;
- Your occupation and business address;
- Financial information including details of your employer, income, name of bank or financial institution;
- Details of your spouse, de facto, and dependent children.
- Details of properties owned by you.

In order to provide services to you, we may disclose your personal information to the persons/organizations described below:

- Your legal advisor(s) and the legal advisor(s) representing the other party(s) involved in your transaction;
- Your financial institution and/or financial advisor;
- Insurance providers and brokers;
- Utility providers and utility connection service providers;
- Persons or organizations involved in providing, managing or administering your shipment or goods including independent contractors engaged by the Bureau.
- Tradespeople engaged by us to repair or maintain a property owned or leased by you;
- Organizations involved in maintaining, reviewing and developing the Bureau's systems, procedures and infrastructure including maintaining or upgrading our computer systems;
- Organizations involved in the payments systems including financial institutions, merchants, and payment organizations;
- Tariff Commission;
- Bureau of Internal Revenue;
- Department of Finance;
- Philippine National Police;
- National Bureau of Investigation;
- Other Government Agencies;
- With third parties because you have given consent.

Whenever it is reasonable or practicable to do so, we will collect your personal information directly from you. Sometimes it will be necessary for us to collect information from a third party or a publicly available source, such as your legal adviser, your past or current employers, your past or current clients, and your past or current brokers or agents.

In the course of providing services to you, it may be necessary for us to enter your personal information into forms generation software and customs websites. Depending on the terms of use of such software and websites, a third party may acquire rights to use or disclose information entered into the relevant forms or websites.

We need your permission to collect, use, and disclose your personal information and we therefore ask that you sign the consent on the first page of this document to indicate your consent.

In the event that you do not consent to the Bureau of Customs collecting and releasing your personal information as described above, we may be unable to provide the services requested by you.

II. Access to, and correction of personal information

You have the right to request access to your personal information and to request that the Bureau update or correct your personal information.

Our privacy policy contains further information about how you may request access to, and correction of, your personal information.

III. Contacting Us

You may contact us by mail, email or telephone as follows:

Mail:

Public Information and Assistance Division (PIAD) Office located at the Office of the Commissioner Building, Gate 3, South Harbor, Port Area, Manila

E-mail:

piad@customs.gov.ph

Telephone:

8705-6000