Quezon City

June 15, 2023

REVENUE MEMORANDUM ORDER NO. 30-2023

SUBJECT: REVISED GUIDELINES FOR INFORMATION ASSET CLASSIFICATION

TO: ALL INTERNAL REVENUE OFFICIALS, EMPLOYEES AND OTHERS CONCERNED

I PURPOSE

The Bureau of Internal Revenue Information Asset Classification Guidelines sets the minimum requirements for information asset security classification. It also provides a standard process to allow offices to evaluate their information assets and determine the appropriate level of security classification that must be applied, addressing the need for a consistent approach to dealing with the sensitivity and confidentiality of information assets across the BIR's network.

By providing a standard approach to information asset security classification, the guideline facilitates improved interoperability and consistency within the BIR's network. The implementation of electronic service delivery has accelerated the need for a consistent approach to security classification, particularly as the BIR seeks to integrate its services and information.

This Order specifies the schema for security classification of information, and related controls that are in accordance with the National Internal Revenue Code (NIRC), BIR's Information Security Policy, Freedom of Information Program (EO No. 2 Series of 2016), BIR's Information Security Manual (RMC No. 128-2019) Data Privacy Act (RA 10173).

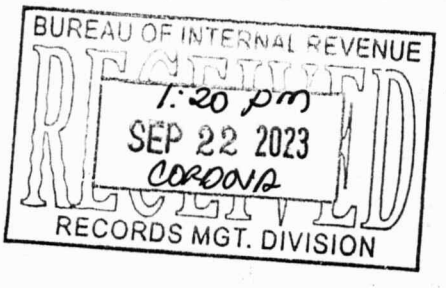
This also aims to harmonize previously issued policies/procedures, specifically: RMO 12-2014 (Implementation of the Information Asset Classification Guidelines) and unnumbered Memo dated November 12, 2018 – (Security Controls in Transmitting Documents in Compliance to RMO 12-2014).

II SCOPE

This Order provides a process and direction for determining the security classification of information assets. This is intended to address the classification of information assets across all delivery mechanisms, including both online services and physical 'over-the-counter' services, and to apply to both electronically and non-electronically stored information. A single guideline for all delivery mechanisms is vital because services and information are increasingly offered on multiple channels.

This will be in particular reference to:

a. Information owners and users who are responsible for the classification and control of BIR's information assets
b. Information asset custodians
c. Any people who are designing BIR services such as business process specialists, application developers, and system architects



d. Business managers and service stakeholders

e. Information security managers and auditors who may assess security of service

f. Heads of Office and employees who have responsibility for managing classified information assets over time and responsible for the supply and operation of information systems

III THE SECURITY CLASSIFICATION SCHEMA

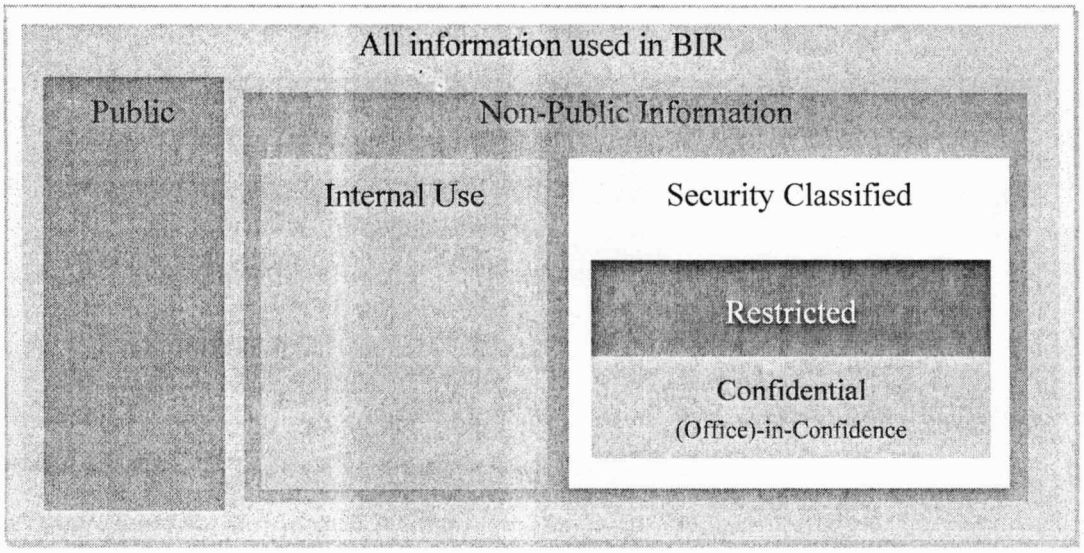
This section outlines the schema to be used for security classification of information assets within BIR. Any information received or collected by, or on behalf of, the BIR through its office and contractors is official information. As it is a valuable official resource, official information:

- must be handled with due care and in accordance with authorized procedures
- must be made available only to people who have a legitimate 'need-to-know' to fulfil their official duties or contractual responsibilities, and
- must only be released in accordance with the policies, legislative requirements and directives of the BIR and the courts.

Official information held within the BIR typically fall into two broad categories:

- Official information intended for public use / consumption; and
- Official information which, because of the adverse consequences of unauthorized disclosure, requires appropriate controls to protect its confidentiality.

The following diagram provides a representation of the various security classifications of official BIR Information.



3.1 PUBLIC INFORMATION

Public information are information assets that has been explicitly authorized by the data owner for wide dissemination or public access through the BIR website, BIR social media accounts, and office email account of the Internal Communications Division or Public Information & Education Division. This classification of information directly relates to the dissemination of information to the public and various stakeholders of the BIR. Such information asset must be clearly labeled as PUBLIC in order to distinguish it from INTERNAL USE information assets.

Although confidentiality is not a requirement of this information asset, it is still necessary to maintain its integrity (accuracy and completeness) prior to its release and availability. Assuring the integrity and availability of a PUBLIC document comes with a cost. As such, an information asset should not be classified as PUBLIC until they are assessed and required to be made available.

Some information assets that require disclosure to the public may have confidentiality requirements before the actual release. As such, the point of the asset's lifecycle, where it needs to be reclassified as PUBLIC, must also be determined and explicitly indicated.

3.2 NON-PUBLIC INFORMATION

Information assets that are classified as non-public can be divided into two categories: internal use and security classified.

3.2.1 Internal Use

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

3.2.2 Security Classified

Security classified information are assets that require a certain degree of confidentiality depending on its potential effect to the BIR. It should be protected with additional security controls as determined by its owner. This classification can be divided into the following:

3.2.2.1 RESTRICTED

The most private and sensitive information asset which requires a substantial degree of protection as compromise could cause serious damage to the BIR and the nation, regulatory or contractual liability, severe damage to operations and loss of public trust and confidence and foreign relationship issues. This type of information classification should be used sparingly as its protection requires a substantial degree of investment. RESTRICTED information assets are usually within the executives (Chief Executive of the Philippines, Department of Finance, Commissioner of Internal Revenue, and the Deputy Commissioners of Internal Revenue).

3.2.2.2 CONFIDENTIAL

Information assets, whose compromise could cause moderate to limited damage to the BIR, should be classified as CONFIDENTIAL. This classification may be used in relation to the Group, Division or Section within the BIR that owns and requires the protection of the information asset.

Examples of CONFIDENTIAL classification may be used as follows:

- PERSONNEL-IN-CONFIDENCE: includes all BIR employee information where access would be restricted to the Personnel Division. Examples are employee evaluations, employee 201 files and grievances.

- AUDIT-IN-CONFIDENCE: includes all audit-related information that are not yet intended or re-classified as PUBLIC document.
- ISG-IN-CONFIDENCE: includes all ISG related information where access would be restricted to the ISG officials and other authorized staff.

3.3 SECURITY CLASSIFICATION ROLE

3.3.1 Information Asset Owner

All information gathered and used by the government agencies are owned by the Republic of the Philippines. This responsibility is passed on to the agencies of the government. For the Bureau of Internal Revenue, the ownership is passed on by the Chief Executive to the Commissioner of Internal Revenue (CIR). The CIR therefore, has the direct authority and accountability over the information asset. The CIR has the responsibility to protect the information asset by ensuring that proper controls are in place.

In order to ensure that proper attention is given to information assets, the Commissioner may further delegate the ownership to the officials of each group and/or division. Information asset ownership should generally be assigned to a BIR Item and not to a natural person to ensure continuity of responsibilities.

The roles and responsibilities of an Information Asset Owner are shown as follows:

- Maintain an inventory of their information assets.
- Perform risk analysis to determine, identify and document the classification of the information assets owned.
- Provide the Security Management Division (SMD) a list of all the information assets identified as confidential and restricted (if applicable).
- Ensure appropriate controls are applied based on the classification of an information asset. More stringent controls for each information asset may be implemented by the owner.
- Authorize access privileges to those needing access to their data.
- Review annually the privileges authorized.
- Determine the retention period of an information asset.

3.3.2 Information Asset Custodian

Information asset custodian has the physical or logical possession of the information asset. They are responsible for the implementation and maintenance of the security controls set by the information asset owner. This is to ensure that confidentiality, integrity and availability criterion is met throughout the information asset's lifecycle. The roles and responsibilities of an information asset custodian are as follows:

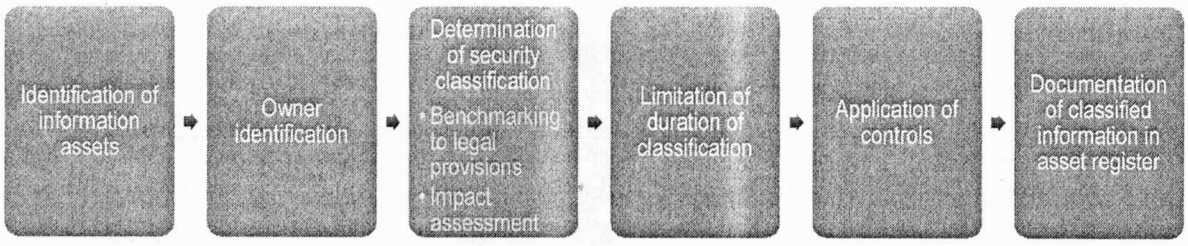
- Implementation of physical and/or logical access control systems to protect the information assets
- Provide and administer general controls such as back-up and recovery systems consistent with the BIR's Information Security Policy and applicable baseline standards.
- Custodians are responsible in establishing, monitoring and operating information systems, containing the information assets of the BIR, consistent with BIR information security policy. This should be in consultation with the information asset owners.
- Custodians should not change or alter the information asset in their custody as well as the agreed security controls unless they have received an explicit authorization from the information asset owner.

3.3.3 Information Asset User

Information Asset User is an individual with explicit authorization to use the information asset. Information Asset User is responsible for implementing controls and executing due care in utilizing information assets. The following are the roles and responsibilities of the information asset user:

- Users should use information only for the purposes specifically approved by the Information Asset Owner.
- Users should comply with all security measures defined by the Information Asset Owner, implemented by the Custodian, and/or defined by the SMD.
- Users should refrain from disclosing information in their possession (unless it has been designated as Public) without first obtaining permission from the Owner.
- Users should report to the Servicedesk all situations, where they believe an information security vulnerability or violation may exist.

IV SECURITY CLASSIFICATION PROCESS



4.1 IDENTIFICATION OF INFORMATION ASSETS

Information assets are data, information or material generated, gathered, compiled, stored or utilized by the Bureau in the conduct of its operations. These include, but are not limited to, taxpayer information, electronic messages, documents, policies, guidelines and procedures.

4.2 OWNER IDENTIFICATION

Each group is responsible for ensuring that information assets are properly classified by the information asset owner and such classification is implemented and maintained by the information asset custodian. Information assets shall be classified by the information asset owner or delegate at the earliest possible opportunity and as soon as the information asset owner is aware of the sensitivity of the information asset. The Information Asset custodian shall ensure that proper care is regarded in handling information assets assigned to them. All assets shall be included in the Bureau's inventory and maintained by the Information Asset Owners and shall have a designated owner and when necessary, a custodian. SMD should be given a copy and keep the complete inventory.

4.3 DETERMINATION OF SECURITY CLASSIFICATION

Security classification of an asset should be based on legal provisions and its impact on the Bureau.

4.3.1 Benchmarking to Legal Provision

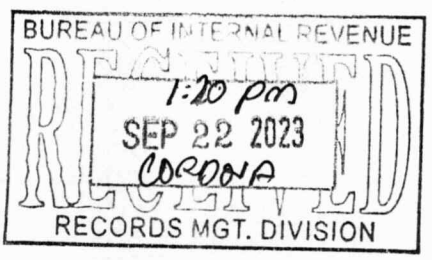
Relevant laws, regulations, issuances, and other references should be considered in determining the classification. The following may serve as basis for classifying the information assets of the Bureau.

a. National Internal Revenue Code
b. Data Privacy Act of 2012
c. Executive Order No. 2 Series of 2016 (FOI Program)
d. Revenue Memorandum Circular No. 128-2019 (People's FOI Manual of the BIR)
e. BIR Information Security Policy

Additional relevant laws, regulations, issuances, or any other reference that eventually becomes applicable should be considered in classifying assets.

Below are legal provisions BIR may use to classify assets based on relevant laws, regulations and issuances.

Legal Provision	Classification	Basis
Information is covered by Executive Privilege	Restricted	BIR FOI Manual (Annex 4, List of Exceptions)
Privileged information relating to National Security, Defense or International Relations	Restricted	BIR FOI Manual (Annex 4, List of Exceptions)
Information concerning Law Enforcement and Protection of Public and Personal Safety	Restricted	BIR FOI Manual (Annex 4, List of Exceptions)
Information deemed confidential for the Protection of the Privacy of Persons and certain individuals such as minors, victims of crimes, or the accused	Confidential	BIR FOI Manual (Annex 4, List of Exceptions)
Information, documents or records known by reason of official capacity and are deemed as confidential, including those submitted or disclosed by entities to government agencies, tribunals, boards, or officers, in relation to the performance of their functions, or to inquiries or investigation conducted by them in the exercise of their administrative, regulatory of quasi-judicial powers.	Confidential	BIR FOI Manual (Annex 4, List of Exceptions)
Prejudicial Premature Disclosure.	Confidential	BIR FOI Manual (Annex 4, List of Exceptions)
Records of proceedings or information from proceedings which, pursuant to law or relevant rules and regulations, are treated as confidential or privileged	Confidential	BIR FOI Manual (Annex 4, List of Exceptions)
Matters considered confidential under banking and finance laws, and their amendatory laws	Confidential	BIR FOI Manual (Annex 4, List of Exceptions)
Other exceptions to the right to information under laws, jurisprudence, rules, and regulations	Confidential	BIR FOI Manual (Annex 4, List of Exceptions)



Legal Provision	Classification	Basis
Sensitive Personal Information may be: 1. About an individual race, ethnic origin, marital status, color and religious, philosophical, or political affiliations 2. About an individual's health, education, genetic or sexual life of a person, or to any judicial proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings 3. Issued by Philippine government agencies peculiar to an individual which includes, but not limited to, Social Security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and 4. Specifically established by an executive order or an act of Congress to be kept classified.	Confidential	Data Privacy Act 2012 (Chapter 1, Section 3)
Information regarding the business, income or estate of any taxpayer, the secrets, operation, style or work, or apparatus of any manufacturer or producer, or confidential information regarding the business of any taxpayer	Confidential	NIRC (Section 270)
Information which compromises or unauthorized disclosure could cause moderate to limited damage to the BIR	Confidential	BIR Information Security Policy (Section 3.3.3)
Information that are generally used in the conduct of the BIR's operations and do not need special security controls which may remain unlabeled and left unclassified	Internal Use	BIR Information Security Policy (Section 3.3.2)
Information that has been explicitly authorized by the owner for public access, through the Internal Communications Division	Public	BIR Information Security Policy (Section 3.3.1)
Information, official records, public records, and documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development	Public	FOI Program (Section 3)
Information on the Bureau's mandate, structure, powers, functions, duties, and decision-making process	Public	BIR FOI Manual (Chapter 4, Section 9)
Information about the Bureau's frontline services and the procedure and length of time they may be availed of	Public	BIR FOI Manual (Chapter 4, Section 9)
Names of the Bureau's key officials, their powers, functions and responsibilities, and their profiles and curriculum vitae	Public	BIR FOI Manual (Chapter 4, Section 9)
Work programs, development plans, investment plans, projects, performance targets and accomplishments, and budgets, revenue allotments and expenditures	Public	BIR FOI Manual (Chapter 4, Section 9)
Important rules and regulations, orders or decisions	Public	BIR FOI Manual (Chapter 4, Section 9)

Legal Provision	Classification	Basis
Current and important database and statistics the Bureau generates	Public	BIR FOI Manual (Chapter 4, Section 9)
Bidding process and requirements	Public	BIR FOI Manual (Chapter 4, Section 9)
Mechanisms or procedures by which the public may participate in or otherwise influence the formulation of policy or the exercise of its power	Public	BIR FOI Manual (Chapter 4, Section 9)

4.3.2 Impact Assessment

If there are no laws, regulations, issuances and other references that could identify the classification of information assets, impact of it being compromised should be considered. An impact assessment matrix may be used as a guide to evaluate the classification of information assets. Below is an impact assessment matrix which may be used by the Bureau.

Impact Criteria	Minor/Negligible	Moderate	Major
Distress caused to any party	No impact	Short term Damage	Long term Damage
Damage to a party's reputation	No impact	Short term Damage	Long term Damage
Public order	No impact	Can cause slight confusion	Can cause chaos
Financial Loss to agency /service provider	No impact	Minor. Less than 2% of monthly budget.	> 2% of monthly budget.
Threat to BIR's systems or capacity to operate	No impact	Can cause slight efficiency issues	Can cause major efficiency issues or total stoppage of operation
Impact on development or operation of major government policy	No impact	Can cause slight confusion	Can cause chaos or failure to operate policy
Potential Information Asset Classification	**Consider for Internal Use/Public**	**Internal Use**	**Confidential**

4.4 LIMITATION OF DURATION OF CLASSIFICATION

Asset classification may vary at a point in time. Duration of classification may be determined up to a specific date or event. An event may trigger an increase or decrease in sensitivity or change in target audience. For instance, a revenue memorandum in its draft state shall be considered CONFIDENTIAL and be classified as PUBLIC on Commissioner's approval. Protection applied to information assets may change when classified or declassified.

4.5 APPLICATION OF CONTROLS

Pertinent controls shall be applied to ensure that appropriate protection is given to information assets in accordance with the determined security classification. Confidentiality, integrity and availability of information shall be considered in applying specific controls on information assets. These controls are outlined in Section 5 of this Order.

4.6 DOCUMENTATION OF CLASSIFIED INFORMATION ASSETS IN REGISTER

BIR should maintain an information asset inventory that records all information assets of the Bureau with corresponding security classification.

Information asset inventory shall be maintained in a centralized location and should cover all information assets of the BIR, readily accessible to BIR Management.

At a minimum, an information asset register should include:

a. Unique identifier of asset (unique control number)
b. Description of information asset
c. Location of information asset
d. Information asset owner
e. Security classification
f. Date of security classification and name of who approved the classification
g. Reason for the security classification

The following may be considered in maintaining an information asset register:

a. Date to review security classification
b. Users and usage of information
c. Number of copies in circulation
d. Disposal details where information has been disposed

In the event that information asset is identified as confidential, the Information Asset Owner should provide copy to SMD and make the necessary updates in the information asset inventory.

V SECURITY CONTROLS

5.1 FILING AND MARKINGS

Information assets are distinguished among information classification through their respective filing and markings. Appropriate protective filing and markings are the following:

Public

- An archive of public documents accessible to the public must be maintained.
- Information must be marked "Approved for Public Release"

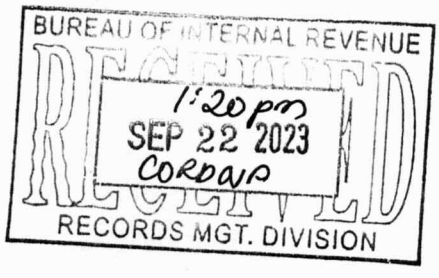
Internal Use

- Information must be marked "Internal Use Information"
- Filing must be in accord with normal records management practices.

Security Classified

- Information must be marked "Restricted" or "Confidential". Additional marking for Confidential information should be labelled to indicate its sub-classification such as "(Office)-in-Confidence"
- Sub-classified information assets must be filed separately, and a distinctive file must be maintained accordingly.

Refer to Annex A and B for sample TOP Sheet for Security Classified Information.



5.2 RECLASSIFICATION OF INFORMATION

Information assets may change its state of criticality and sensitivity. Therefore, information assets may be reclassified at a point in time or when necessary. For instance, public information may be held confidential prior to its release. Any reclassification must be done by the information asset owner. Reclassification may be considered in the following scenarios:

- A legal, legislative, regulatory, policy or any other provision requires reclassification of the information asset.
- There is a change in the state of information (e.g., criticality, sensitivity).
- Significant changes occurred affected the impact of information assets (e.g., change of government, change strategic priorities).
- The user believes that there is a need to reclassify the information asset. User must advise the information asset owner who may consider the reclassification.

In the event that the information asset changes and become confidential, the Information Asset Owner should provide copy to SMD and make the necessary updates in the information asset inventory.

5.3 MINIMUM BASELINE CONTROLS

Appropriate controls must be established to ensure that appropriate protection is applied to information assets. Controls are applied according to the determined asset classification.

5.3.1 Public Information

a. Available to the public
b. Information accessed by the public should not be modifiable. Modifications and updates are limited to information asset owner
c. Contents to be published are authorized by the Internal Communications Division

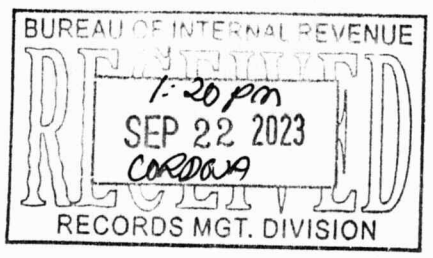
5.3.2 Internal Use Information

a. Available within the Bureau
b. Available to any employee or third party (e.g., vendor, consultants, other government agencies, AABs, OJTs) upon approval from the immediate head or, if appropriate agreements are in place, an employee who can disclose or share this information with the extended enterprise
c. Default privilege is read-only

5.3.3 Security classified information

5.3.3.1 Restricted

a. Access is limited to those approved by the Commissioner
b. Information is not disclosed to extended enterprises
c. Modifications and updates are limited to the information asset owner
d. Electronic documents should be encrypted while in transit, and at rest with storage level encryption
e. Strong authentication method should be applied to devices containing electronic documents



5.3.3.2 Confidential

a. Access is given to a limited audience within the Bureau
b. Information is disclosed to an extended enterprise with appropriate agreements in place
c. Modifications and updates are limited to the information asset owner
d. Electronic documents should be protected both while in transit and at rest.
e. Strong authentication method should be applied to devices containing electronic documents

5.4 NON-GENERAL SECURITY CONTROLS

5.4.1 Discussing security classified information

Discussions of security classified information should be taken with care to ensure that leakage is prevented from people without a need-to-know. The following shall be observed in conducting meetings involving security classified information:

a. Meetings should occur behind closed doors ensuring area is secured
b. Roster of attendees should be approved by the information asset owner
c. Meeting materials should have classification markings
d. Information written on whiteboards or stored on equipment should be removed prior to vacating the meeting room

5.4.2 Video Conferencing

Video conferencing as a medium to communicate must be done thru approved applications (Zoom, Teams, etc.). Personnel utilizing video conferencing using BIR's IT assets must adhere to the Bureau's Acceptable Use Policy (AUP). In addition, when using Zoom or Teams or any means of video conferencing, the conference host must obtain the consent of the participants within the call prior to initiating any recording. The recording shall be classified based on the information discussed on the conference, and as guided by the information asset classification guideline.

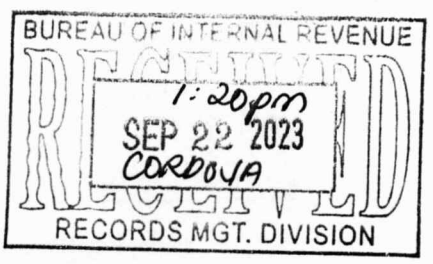
5.4.3 Copying Non-Public information

Copying of Non-Public information may be prohibited by the information asset owner. Copies of the information should be numbered and labelled per information asset classification.

5.4.4 Storage of classified information

Physical documents should be stored and locked in secure locations. The clean desk policy should always be practiced. Other security controls may be applied as by prescribed by the Bureau.

For electronic documents, access should be restricted and specific security controls should be implemented depending on the container (e.g., workstation, portable media device, cloud storage, etc.) of the electronic document, as prescribed by the Bureau.



5.4.5 Electronic authentication and access

Access to information should be validated through electronic authentication. Information should be protected with a strong password in compliance with the Password and Login Control Guidelines at the minimum. Additional authentication mechanisms that may be implemented are as follows but not limited to:

a. Tokens
b. Biometrics
c. Access badge
d. Radio-frequency Identification (RFID)

5.4.6 Audit logs

Audit logs should be enabled in the system. Monitoring of audit logs should be conducted regularly.

5.4.7 Digital transmission

- Data Transmission

  Information may be passed over appropriately classified internal networks (e.g., SFTP, Sharepoint) or external networks (e.g., the internet, virtual private networks (VPNs), or cloud-based services). Information should be encrypted during transmission to organizations outside the BIR.

- Email

  Email messages containing non-public information should be sent to recipients on a need-to-know basis, it must be appropriately labelled based on the classification, encrypted, and a digital signature must be enabled for additional authentication. Contents and attachments should be encrypted or password protected. Additionally, for security classified information, emails should be labelled with "Restricted" or "Do Not Forward" to prevent unauthorized sharing or dissemination of the information.

5.4.8 Physical transmission

- Within the Bureau

  Documents should be sealed in an opaque container (e.g., envelope, box, etc.) indicating its classification. It should not be left unattended on recipient's desk. There must be a confirmation from recipient upon delivery of authorized BIR personnel/messenger.

- Outside the Bureau

  Document should be sealed in double containers. Sealed inner and outer container should indicate its classification. It should not be left unattended on recipient's desk. Documents should be sent via registered mail, accredited courier service, or by authorized BIR personnel/messenger with confirmation of receipt.

5.4.9 Retention, Archiving and Disposal

- Electronic Documents
  a. Information should be retained based on the retention period defined by the information asset owner.
  b. After the defined retention period, the information should be deleted immediately.
  c. Prior to disposal, the media/container should be cleared of all data and or physically destroyed.

- Physical Documents
  a. Information should be retained based on the retention period defined by Revenue Memorandum Circular No. 73-2008 for BIR Records Disposition Schedule.
  b. After the defined retention period, shred all documents and files or place in secure receptacle for future shredding. Refer to Revenue Memorandum Order No. 21-2023 for Policies, Guidelines and Procedures in the Disposal of Valueless Records in the Bureau of Internal Revenue (BIR).

VI NON-COMPLIANCE

Non-compliance with the information security policies, standards, guidelines and procedures shall subject the offender to immediate disciplinary and/or legal actions.

VII REPEALING CLAUSE

This Order supersedes RMO 12-2014 and other related issuances, memoranda, guidelines and/or portion thereof inconsistent herewith.

VIII DOCUMENT MANAGEMENT AND MAINTENANCE

SMD and ITPSD are responsible for the management, maintenance and accuracy of the guidelines. Any questions regarding the guidelines should be directed to the SMD.

IX EFFECTIVITY

This Order shall take effect immediately.

ROMEO D. LUMAGUI, JR.
Commissioner of Internal Revenue
014390

BUREAU OF INTERNAL REVENUE
RECEIVED
1:20 pm
SEP 22 2023
CORDOVA
RECORDS MGT. DIVISION