IAM Policy Document Issue Version: 1.0

|  |  |
| --- | --- |
| Version Number: | 1.0 |
| Document Release Date: | 12/20/2022 |
| Security Classification: | Protected |
| Author: | Larry W. Wilkes II |

**Information Asset Management Policy**

IAM Policy Document Issue Version: 1.0

**Document Control**

|  |  |
| --- | --- |
| Item | Description |
| Doc. ref | Version 1.0 |
| Classification | Version 1.0 |
| Release Date: | 12/20/2022 |
| Revision Date: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Author(s) | Remarks |
| 1.0 | Dec 20 2022 | L.Wilkes |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Review and Approval History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Approver(s) | Remarks |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

IAM Policy Document Issue Version: 2.0

Table of Contents

1. Introduction ...................................................................................................................................... 4 1.1. Purpose .......................................................................................................................................... 4 1.2. Scope ..............................................................................................................................................4 1.3. Information Assets..........................................................................................................................4

2. Asset Inventory ............................................................................................................................... .4 2.1. Information Asset Register........................................................................................................... 4 2.2. Asset Value-Based Approach........................................................................................................ 5

3. Information Classification ............................................................................................................ 5 3.1. Classification Scheme .................................................................................................................. 5

4. Acceptable Use of Assets ............................................................................................................... 6 4.1. Authorization of Use .....................................................................................................................6 4.2. Return of Assets ............................................................................................................................6

5. Asset Disposal ................................................................................................................................. 6 5.1 Secure disposal ...............................................................................................................................7

6. Roles and Responsibilities............................................................................................................ 7 6.1. Information Asset Owner ............................................................................................................. 7 6.2. Information Asset Custodian........................................................................................................ 7

IAM Policy Document Issue Version: 2.0

**1. Introduction**

**1.1. Purpose**

The purpose of this policy is to outline The Govt’s information asset management policy and the actions that will be taken to provide sufficient maintenance of the Information Asset Register. The policy details the requirements and responsibilities of officers for updating and ensuring accurate representation. This policy also provides a framework to ensure its vital information assets are accounted for and managed appropriately and according to statutes, regulations, and government policies.

**1.2. Scope**

The Information Asset Register and supporting action plan covers all The Govt employees and its contractors/providers to manage information assets.

**1.3. Information Assets**

An information asset can be defined as;

-an operating system

-infrastructure

-business application

-off-the-shelf product

-user-developed application

-records

-information

-IT hardware

It will have recognisable and manageable value, risk, content and lifecycles and can range from a basic Excel spread sheet or database to a national system. The information asset register is defined as a centralised log of all information that is held by the departments within The Govt but not limited to the nature of the data (i.e., personal or sensitive), what information is held (i.e. names, addresses etc.) but also both electronic and physical locations of the information.

**2. Asset Inventory**

**2.1. Information Asset Register**

It is a core information governance objective that all organization’s information assets are recorded in a comprehensive information asset register. Information asset register is an inventory maintained by individual Information Asset Owners from relevant departments within The Govt and coordinated by the Information Asset Lead.

Specific details are required to manage and account for each asset successfully. Each asset must have at least the following information in the Information Asset Register to be meaningful.

a. Asset Name

b. Asset Type/Category

c. Asset Owner

d. Asset Custodian

e. Location

2.2. Asset Value-Based Approach

An asset value is given to each asset according to its impact on The Govt as estimated by IAO. The value is either Low(1), Moderate(2), High(3) or Very High(4), and they are measured using the valuation types below.

a. Confidentiality

b. Integrity

c. Availability

Using this approach, IAO can sum up an Overall Asset Value to determine the sensitivity and importance of their asset, allowing them to plan and mitigate risks in events of assets being compromised.

A sample Information Asset Register document can be found in internal SharePoint.

**3. Information Classification**

On creations, all owners must assess and classify their information assets according to their content. The classification determines how the document should be protected and who should be allowed to access it.

**3.1. Classification Scheme**

The Govt’s information classification scheme requires information assets to be protectively marked into one of the three classifications (excluding Unofficial information, which does not need to be marked). The way the document is handled, published, moved and stored will be dependent on this scheme.

The classes of information are:

a. Unofficial

* **Public**: This information is public information, and can be openly shared on your website, discussed in public and with anyone. Public information as the name implies, is public, and does not require any additional controls when used.
* **Internal**: Internal information is company-wide and should be protected with limited controls. Internal information may include the employee handbook, various policies and company-wide memos. If disclosed, Internal information has a minimal impact to the business.
* **Confidential**: Confidential information is team-wide and its use should be contained within the business. This information may include pricing, marketing materials, or contact information. If disclosed, Confidential information could negatively affect your business and ultimately your brand.
* **Restricted**: Restricted information is highly sensitive and its use should be limited on a need-to-know basis. Restricted information is typically protected with a Non-disclosure Agreement (NDA) to minimize legal risk. Restricted information includes trade secrets, potentially identifiable information (PII), cardholder data (credit cards), or health information. If disclosed, there would be a significant financial or legal impact to the business.

The definition of these classes of information is described in further details in the Information Asset Register document. The decision regarding which classification an information asset should fall into is based on the following main criteria:

1. Legal requirements that must be complied with

2. Value to the organization

3. Criticality to the organization

4. Sensitivity to unauthorized disclosure or modification

All electronic documents shall be labelled according to the four classes described above

**4. Acceptable Use of Assets**

All employees, contractors and service providers of The Govt must use The Govt assets:

1. For the purposes they were acquired; and

2. With care and in a manner that ensures the asset is subjected to the minimum wear and tear or damage.

If you handle official, protected or secret information, you must take all reasonable steps to safeguard it.

· Users must observe The Govt’s Information Security policies and guidance, particularly concerning removable storage media, mobile and privately owned devices.

· Users must not infringe copyrights or break the terms of software licenses and other materials

· Users must not attempt to access, delete, modify or disclose Information Assets belonging to other people without their permissions unless it is evident that they intend others to do this.

**4.1. Authorization of Use**

· Users may only access those Information Assets for which they have explicitly authorized by the asset owner.

· Access to The Govt Information Assets will only be granted to duly authenticated users through a unique user name and password policy as stated in the Password Policy guideline.

**4.2. Return of Assets**

Upon termination of an employment contract or other contract based on which various equipment, software or information in electronic or paper form is used, the user must return all such information assets to his/her line manager or the asset owner.

**5. Asset Disposal**

Asset and media disposal may appear to be simple activities since we generally only dispose of things that we deem no longer needed or not valuable. However, sometimes, what is worthless to someone can be highly valuable to someone else.

The same applies to information. Some information we consider not valuable can lead a competitor to gain a business advantage or, worse, a criminal to explore an organization’s weaknesses and cause damage.

**5.1 Secure disposal**

To ensure the proper and secure disposal of the information asset,

1. Disposal procedures should be proportional to the information classification: the higher the classification, the greater assurance that information cannot be retrieved after disposal. Some examples of good practice are shredding the media or overwriting the data.

2. Clear identification of information requiring secure disposal: Use a watermark for easy and clear identification.

3. Keep traceability of sensitive disposed items: Users who performed the disposal procedure must keep a log on the information disposed of and what method was used.

6. Compliance and Violations

In protecting its information assets, The Govt will comply with all applicable laws and regulations. The Govt” requires its employees to meet the highest ethical standards in dealing with clients, vendors and other government agencies when in possession of the information assets.

The responsibility for protecting and securing vital information assets rests with all Company employees. This responsibility is shared with third parties under the same obligation to protect The Govt information assets.

Failure to comply with The Govt’s information asset management policy will result in disciplinary action and/or contractual rights, remedies and actions by the Govt.

**6. Roles and Responsibilities**

**6.1. Information Asset Owner**

Under their job descriptions, Heads of Departments or their authorized representatives must act as the Information Asset Owner for their service areas.

Purpose of the Role:

· Determine information sensitivity and create/fill up asset inventory (information asset register);

· Maintains an understanding of ‘owned’ assets and how they are used;

· Approves and minimizes information transfers while achieving business purposes;

· Oversees the disposal mechanisms for the information asset when no longer needed;

· Knows what information the asset holds and who has access to update the system;

· Undertakes regular reviews on the information risk associated with the asset;

**6.2. Information Asset Custodian**

Custodians refer to any individual in The Govt who has physical or logical possession of the information asset. They can be from different departments within The Govt who has a vested interest in the specific information assets they use.

Purpose of the Role:

· Protect an information asset as it is stored, transport or process in line with the requirements defined by the Information Asset Owner;

· Ensure the security of the information and adhere to all information security policies, standards and procedures;

· Document all the information security controls implemented and share them with the Information Asset Owner