POLICY

| ITWORKS | 184

|  |  |  |
| --- | --- | --- |
| **Title** | Information Classification and Handling Policy | |
| **Version Approved** | IT WORKS Executive | Version Active Date: 30 May 2018 |

**Contact Officer**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Peter Perfect | Phone | (08) 8000 0000 |
|  |  |  |  |
| Position Title | Manager – Service Delivery | | |
|  |  |  |  |
| Email Address | perfectp@itworks.com.au | | |

Table of Contents

[1 Policy 2](#_Toc527537733)

[2 Scope 2](#_Toc527537734)

[3 Definitions 2](#_Toc527537735)

[4 Related policies 2](#_Toc527537736)

[5 Procedure 3](#_Toc527537737)

[5.1 Information assets 3](#_Toc527537738)

[5.2 Why information classification is important 3](#_Toc527537739)

[5.3 The Information Classification Lifecycle 3](#_Toc527537740)

[5.4 Information Asset Classification and Control 3](#_Toc527537741)

[5.5 Information labelling and handling 4](#_Toc527537742)

[5.6 Information Labelling Implementation Approach 4](#_Toc527537743)

[5.7 Information Owners 4](#_Toc527537744)

[5.8 Information Asset Custodian 5](#_Toc527537745)

[5.9 Manager ICT Business and Assurance, ICT Services 5](#_Toc527537746)

[6 Responsibilities 5](#_Toc527537747)

[6.1 Specific responsibility of IT WORKS staff 5](#_Toc527537748)

[6.2 Review of this Policy 5](#_Toc527537749)

[7 Appendix A: Information Classification Scheme 6](#_Toc527537750)

# Policy

|  |  |
| --- | --- |
|  | IT WORKS information will be classified to suitably reflect its importance, degree of sensitivity and protection requirements and such classification should be periodically reviewed.  Once assigned a classification, the information must be appropriately handled to adhere to protection controls for confidentiality, integrity and availability as well as any other special handling measures applicable to the defined classification of the information. |

# Scope

|  |  |
| --- | --- |
|  | This procedure applies to all information and information processing facilities.  IT WORKS information does not lie within the national security domain. As a result, it is expected that protective marking requirements for national security classified information assets are not applicable and as such they are out of scope for this Policy. |

# Definitions

|  |  |  |
| --- | --- | --- |
|  | Information Asset | An information asset is defined as anything that processes, stores or communicates information of value to IT WORKS, and include the logical groupings of information residing on the hardware domains that have a common business use or purpose. |
|  | Business Owner | A Business Owner is the person or group that is ultimately responsible for an information asset. Individual business units own business critical information and the manager of the business unit responsible for the creation of any information and / or the business unit directly impacted by the loss of confidentiality, integrity or availability of the information is usually the Business Owner. |
|  | Information Asset Custodian | An Information Asset Custodian is the person or group that take responsibility for the ongoing management of the information assets (such as a CIO or system administrator). Information Asset Custodians do not own business critical information. |

# Related policies

|  |  |  |
| --- | --- | --- |
|  | ITWORKS/171 | IT WORKS Information Security Policy |
|  | ITWORKS/186 | IT WORKS ICT Remote Access Security Policy |
|  | ITWORKS/170 | IT WORKS Cyber Security Incident Reporting Policy |
|  |  |  |

# Procedure

|  |  |
| --- | --- |
|  | This procedure outlines the obligations of IT WORKS staff in relation to the classification, handling and labelling of information assets in accordance with its security requirements. |

## Information assets

Information assets are critical to every organisation and are essential elements in achieving business objectives and goals. Information assets include anything that processes, stores or communicates information of value to IT WORKS, and include the logical groupings of information residing on the hardware domains that have a common business use or purpose.

## Why information classification is important

Classification of information assets ensures that they are suitably labelled and protected based on their importance and degree of sensitivity, and should be considered when modifying or implementing new information systems. The framework outlined in the IT WORKS Information Security Policy underpins the consistently high classification standards required for all information assets, including student records and other IT WORKS information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

## The Information Classification Lifecycle

Information classification, handling and labelling is an ongoing process that helps to ensure alignment of security controls with information asset classifications. An effective information classification scheme relies on a series of steps that include:

* Identification of information assets and assignment of ownership
* Classification of information assets based on consideration of the risks and impact of loss of confidentiality, integrity and availability
* Implementation of controls to adequately protect information assets based on their classification, including handling and labelling procedures
* Maintenance of an information asset register
* Training and awareness.

## Information Asset Classification and Control

All information assets shall be clearly identified and have a nominated Business Owner and Information Asset Custodian.

The Business Owner of the information asset, in coordination with the Manager ICT Business and Assurance, shall be responsible for classifying the information asset based on the risks related to loss of confidentiality, integrity and availability in accordance with Appendix A – Information Classification Scheme.

All information assets and their Business Owner, Information Asset Custodian and classification shall be clearly recorded within the IT WORKS Information Asset Register maintained by the Manager ICT Business and Assurance. The IT WORKS Information Asset Register forms part of the Configuration Management Database (CMDB) maintained by ICT Services.

The Business Owner of the information asset, in coordination with the Manager ICT Business and Assurance, shall be accountable for ensuring that the security of the information asset is maintained at the appropriate level through an understanding of risks associated with the information asset and application of controls to ensure adequate protection. Responsibility for implementing and managing controls may be delegated, although accountability must remain with the nominated Business Owner.

The Information Asset Custodian, in consultation with the Business Owner and Manager ICT Business and Assurance, should identify the controls to be implemented to provide appropriate levels of physical and logical protection for the information asset.

The addition or removal of an information asset shall be communicated to the Business Owner and Manager ICT Business and Assurance in a timely manner so it can be appropriately classified/declassified and added/removed from the Information Asset Register. Events that may require classification/declassification include the development or acquisition of new information systems, and information with confidentiality requirements that will no longer be required when it is released to the public in the future (e.g. Budget papers).

The Information Asset Register shall be reviewed at least annually by information asset Information Owners in coordination with the Manager ICT Business and Assurance to ensure it is accurate and complete.

Information received from another Agency or Australian jurisdiction shall be protected according to the classification applied by the originating Agency.

## Information labelling and handling

All information assets should be physically or electronically labelled in accordance with the corresponding information asset classification as defined in Appendix A – Information Classification Scheme.

All information assets shall be maintained, handled, stored, transported (or transmitted) or destroyed based on information asset classification labels and relevant information security policies and procedures.

Information classified by another Agency or Australian jurisdiction shall not have its classification modified or removed without express written permission from the Business Owner in the originating Agency or jurisdiction.

Information in production databases must not be used in testing or development databases unless the testing or development environments are secured to the same security standard as the production environment.

## Information Labelling Implementation Approach

IT WORKS has adopted a staged approach to mandating the labelling of information. Labelling is mandatory for the documents listed on the Governance and Research/ Document Classification and Labelling intranet page; however staff are encouraged to apply these guidelines to all IT WORKS documents.

## Information Owners

Information owners have the following responsibilities under this Policy for their information assets:

* Maintain an understanding of owned information assets, including what information they hold, how they are used and who has access to modify them.
* Classify owned information assets in coordination with the Manager ICT Business and Assurance according to the risks related to loss of confidentiality, integrity and availability.
* Ensure owned security of information assets are maintained at the appropriate level through the implementation and management of appropriate controls. Responsibility for implementing and managing controls may be delegated, but accountability remains with the Information Owner.
* Periodically review information assets owned in coordination with the Manager ICT Business and Assurance to ensure the Information Asset Register remains accurate and complete.
* Ensure information classification, handling and labelling policies, procedures and standards are followed.
* Ensure all staff receive adequate user awareness training based on the information assets used in their job role through collaboration with the Manager ICT Business and Assurance as required.
* Approve and oversee the disposal of information assets no longer needed in accordance with IT WORKS information disposal policies and procedures.

## Information Asset Custodian

The Information Asset Custodian has responsibility to manage information assets on an ongoing basis, ensuring that they are adequately protected through implementation and management of appropriate controls that have been agreed with the Information Owner and Manager ICT Business and Assurance.

## Manager ICT Business and Assurance, ICT Services

The Manager ICT Business and Assurance has the following responsibilities:

* Understand how strategic business goals of IT WORKS may be impacted by information asset risks
* Ensuring information assets are:
* Identified
* Assigned ownership
* Prioritised based on a risk and impact assessment
* Appropriately classified as described in this Policy
* Appropriately protected by ICT and business controls including handling and labelling requirements
* Documented in the Information Asset Register
* Periodically reviewed to ensure the Information Asset Register remains complete and accurate
* Maintain information classification, handling and labelling policies and procedures
* Maintain the Information Asset Register
* Ensure actual and potential security incidents and threats are recognised and appropriately addressed

# Responsibilities

## Specific responsibility of IT WORKS staff

All IT WORKS staff are required to comply with the Information Security Policy and related policies, procedures and standards of IT WORKS, the Code of Ethics, and to play an active role in protecting information assets.

All IT WORKS staff have the following responsibilities for information classification and handling:

* Maintain an understanding of information classification, handling and labelling policies, procedures and standards.
* Handle and label information assets in accordance with classification requirements.
* Support the operation of information security controls to maintain an adequate level of protection for information assets.
* Identify and report information security incidents.

## Review of this Policy

IT WORKS Policy must be reviewed at least every two years, but may be actioned earlier according to strategic priorities, reforms or feedback received.

# Appendix A: Information Classification Scheme

The following sections provide a reference for determining an appropriate classification based on the risk of loss of confidentiality, integrity and availability, which is compliant with the ISMF and PSPF.

**Confidentiality**

Confidentiality is evaluated based on the extent of business impact caused by an unauthorised disclosure of the information asset.

All information not in the public domain should be considered for ‘official use only’ and only accessed by personnel who legitimately need it to carry out their official duties. Information with confidentiality requirements that will be released to the public domain in the future (e.g. Budget papers) should specify the date of release, and when the confidentiality requirements cease IT WORKS will continue to consider ongoing integrity and availability requirements.

As IT WORKS are not expected to create or handle information that is sensitive from a national security perspective, the use of protective markings is not expected to applicable. However, if a new or modified information asset is considered to lie within the national security domain, it should be classified in accordance with PSPF requirements.

The table on the following page defines the confidentiality valuation matrix:

|  |  |
| --- | --- |
| **Confidentiality Valuation Matrix DLM** | **Description** |
| **[SLC]**  Sensitive: Legal or Commercial  **[SM]**  Sensitive: Medical | Compromise could cause *moderate damage* to the State, the Government, commercial entities or members of the public.  Sensitive: Commercial should be used with information that may give unfair advantage to a company or is commercially confidential.  Sensitive: Legal should be used for any information that may be subject to legal professional privilege (held or generated by the South Australian Government).  Sensitive: Medical [SM] should be used for any information that may be subject to medical practitioner-patient privilege, or where secrecy provisions of healthcare enactments or other medical industry legislation may apply. |
| **[SOUO]**  Sensitive: Office Use Only  **[SP]**  Sensitive: Personal | Compromise could cause *limited damage* to the State, the Government, IT WORKS, commercial entities or members of the public.  Sensitive official use only [SOUO] should be used in  place of [FOUO] with security classified or unclassified information: where the secrecy provisions of enactments may apply, and/or the disclosure of which may be limited or prohibited under legislation.  Sensitive: Personal should be used with security classified or unclassified information that includes sensitive personal information. An example of this could be academic, financial and health status information included in student records. |
| **[FOUO]**  For Official Use Only | For Official Use Only [FOUO] should be used with unclassified information containing no personally identifiable information (i.e. privacy data). |
| **Public** | Information authorised for unlimited public access and circulation, such as IT WORKS publications and web sites. Such information should still be accompanied by Integrity and Availability classifications. |

**Integrity**

Integrity is evaluated based on the extent of business impact caused by inaccurate and/or incomplete information and/or processing methods of the information asset. The following table defines the integrity valuation matrix:

|  |  |
| --- | --- |
| **Classification** | **Description** |
| **I4** | ABSOLUTE requirement, implying that no inaccuracies or omissions can be tolerated. |
| **I3** | HIGH requirement, meaning that a loss of integrity would cause significant embarrassment and disruption and might be difficult to detect. |
| **I2** | MODERATE requirement, meaning that IT WORKS would be somewhat affected by a loss of integrity, but the situation could be easily detected and recovered. |
| **I1** | LOW requirement, such that there would be minimal |

**Availability**

Availability is evaluated based on the extent of business impact caused due to unavailability of the information asset to authorised users when required. The following table defines the availability valuation matrix:

|  |  |
| --- | --- |
| **Classification** | **Description** |
| **A4** | ABSOLUTE requirement, meaning that IT WORKS would be crippled by the loss and recovery must be virtually instantaneous (no longer than a few minutes). |
| **A3** | HIGH requirement, meaning that loss would cause major disruption to IT WORKS and recovery must be achieved within a period measured in hours. |
| **A2** | MODERATE requirement, implying the loss would have a significant impact and recovery must be achieved within a period measured in days. |
| **A1** | LOW requirement, meaning that loss of the data or service would have only a minor impact on IT WORKS for an extended period. |