1/033 Information Classification Policy

Objective

The objective of this policy is to provide the Town of Port Hedland (the Town) with an information classification framework that enables the Town to label information according to its sensitivity. Information will be identified for its sensitivity and protective security measures applied and communicated within the Town, with other Local Government agencies, and third-party organisations (where relevant). This will build trust for information sharing by using widely understood labels and increase the literacy and awareness of the Town workforce.

Content

Scope

This policy applies to all information received, created, managed, or shared by the Town of Port Hedland.

Information and data will be defined as one of three essential classifications for security compliance and to establish a basic, common language across the Town and government.

These are:

UNOFFICIAL – information which is unrelated to the official work of the Town.

OFFICIAL – is the appropriate classification for most of the information created, used, or managed/received by the Town, and include content related to routine business operations and services and may include emails, briefing notes, draft policies, and guidelines on issues deemed to be non-sensitive.

OFFICIAL: Sensitive – Is the highest level of classification for information that is not covered under arrangements with other authorities. Release of this information could result in damage to individuals, organisations, or government. Includes Human Resources documents and tender documents.

Classification of information above *OFFICIAL: Sensitive* is outside the scope of this policy. Refer to the provisions of the relevant inter-jurisdictional agreement(s) regarding information at higher classification levels e.g., COMMONWEALTH SECURITY CLASSIFIED information.

The Policy does not provide direction on digital security measures to protect information. This is provided through the Information Management Policy.

Responsibilities

The Town will provide direction to all employees, including full-time, part-time, or casual, sessional, fixed term and other contractors on their responsibilities for maintaining proper standards for creation, management, maintenance and retention of Information Classification.

This policy is applied:

- to prevent the unauthorised disclosure of official papers or documents supplied to or seen by Elected Members, staff or contractors in their official duties.
- when information is created, altered, or received. The originator or owner is responsible for conducting an information classification assessment and applying labels as appropriate. Labels must be applied to information such that the label is clear, and wherever possible, prior to subsequent users accessing the information (e.g. a label in the header of an email; a clear marking at the top of a page).
- when Town information is shared within or between the Town and other agencies. The owner of the information is responsible for determining the classification. Town employees and contractors may not change the classification of information without the permission of the party they receive it from.
- to ensure any party having access to the information is aware of and adheres to the Policy requirements.
- prior to any planned release of information, re-assess the information to account for the context of the release (e.g. information being shared in combination with other information which may combine to alter its significance); and
- prior to transition to innovative technology infrastructure based on sensitivity of information.

The information classification process is part of core business and planning, not the delegated responsibility of ICT teams.

The Town is not required to conduct a classification process on existing information or groups of information, until they are used (and then, in line with the Towns staged transition approach).

Risk Management

Information classification is primarily a risk management activity. Risks to information are those that impact the authenticity, reliability, integrity, and useability of the information. The Town will identify and mitigate risks to its information systems and assets.

The Town will take a risk-based decision-making approach to information security and sharing of information. To enable this approach the Town will regularly review and document it is information assets. It will implement the appropriate level of classification to all information, its processes, and systems.

Definitions

"Data" raw, unorganised, and organised material such as characters, text, words, numbers, pictures, sound, or video. It may be stored by both digital and non-digital means. Technically, data is a broader term than information, but "information classification" is preferred, as "information" is more commonly used in non-ICT contexts.

"Information" organised, processed, or structured data. The term "information" can be taken to refer to both data and information for the purposes of the Policy.

"Information Assets" an identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions, thereby satisfying a recognised agency requirement.

"Information Classification" a business-level process whereby the sensitivity of a piece of information (or collection of information) is evaluated, and a classification label applied to it if appropriate, such that the sensitivity will be clear to those who access it subsequently.

"Security Classification" Information that has been security assessed as having a business impact level (BIL) of high, or above for potential compromise of its confidentiality. This results in a security classification as a protective marking.

Security classifications include PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET.

"Sensitivity" the severity of negative consequences that are likely to result from the release of information. Sensitivity increases in line with the severity of the potential consequences.

"Release" the making of information accessible to other individuals or organisations within and external to the agency responsible for the information, whether intentionally or unintentionally.

"Label" a text addition to any given information, which represents its classification or sensitivity, such that it is clear to those who access the information.

Relevant legislation	▪ State Records Act 2000. ▪ Local Government Act 1995 ▪ Freedom of Information Act 1992 ▪ Privacy Act1988
Relevant Standards	▪ SA/SNZ TR 18128:2015 ▪ AS/NZS ISO 31000:2018 ▪ Office of Digital Government ▪ State Records Office of Western Australia State Records Commission Standards
Delegated authority	Senior Records Officer
Business unit	IT & Program Delivery
Directorate	Corporate Services

Supporting Documents
Information Classification Procedures
Information Asset Register

Related Documents
Risk Management Policy.
Records Management Policy
Information Management Policy.
Privacy Policy.
Data Breach Policy.

Governance to complete this section			
Version Control	Version No.	Resolution No.	Adoption date
	Version 1.0	CM202425/192	27 November 2024
Review frequency	Annually		

Document Control Statement *– The electronic reference copy of this Policy is maintained by the Governance Team. Any printed copy may not be up to date and you are advised to check the electronic copy at http://www.porthedland.wa.gov.au/documents/public-documents/policies to ensure that you have the current version. Alternatively, you may contact the Governance Team.*