CORPORATE POLICY STATEMENT NO. 7

INFORMATION QUALITY MANAGEMENT

September 2022

1. OBJECTIVE

To establish the guiding principles for information quality management.

2. SCOPE

This policy statement applies to the Department of Biodiversity, Conservation and Attractions (the department), including the statutory authorities of the Botanic Gardens and Parks Authority, Rottnest Island Authority and Zoological Parks Authority (known collectively as the department).

The policy applies to all forms of information assets (past and future) owned and managed by the department.

This policy sets out the principles for information management and assigns the broad responsibility for information quality within the department. The overarching principles of this policy will be operationalised by technical and management activities to achieve information quality.

This policy does not extend to information security which is provided for in the department's Corporate Policy Statement No. 70: Information Security Management.

3. CONTEXT

The department creates, captures and collects a vast variety of information in the course of its activities. This information is an important strategic asset and a source of significant value to the department when managed effectively.

By taking a strategic approach to information management, the department can unlock the value of information to innovate, influence business processes and decision-making, and organisational performance.

Information quality principles set the foundation for a consistent approach to increase the value of information across the department and public sector. Information quality is achieved through the following criteria:

- intrinsic – the extent to which information values are in conformance with the actual or true values;

- contextual – the extent to which information is applicable to the task of the user and is presented in an intelligible and clear manner recognising that information quality depends on the context of use; and

- accessibility – the extent to which information is available or obtainable and appropriately protected.

4. LEGISLATION

The implementation of this policy is consistent with, and will operate within any applicable legislative, policy and strategic frameworks. This includes but is not limited to:

- *State Records Act 2000;*
- *Freedom of Information Act 1992*;
- *Public Sector Management Act 1994*;
- *Privacy Act 1998*;
- Western Australian Information Classification Policy;
- Western Australian Open Data Policy;
- Western Australian Interoperability Policy;
- WA Enterprise Architecture Framework;
- Corporate Policy Statement No. 63: Information and Related Technology;
- Corporate Policy Statement No. 70: Information Security Management;
- the department's Digital and IT Strategy; and
- DBCA Enterprise Architecture Framework for IT.

5. POLICY

The following guiding principles are critical enablers for information quality:

5.1   Information is valued as a strategic asset that is aligned to business needs and community outcomes and is proactively managed to maintain and maximise value from its use.

5.2   Information is 'born digital' and managed within a well-formed information asset lifecycle that considers the whole information continuum[1].

5.3   The department will propagate valuable, dependable and compliant information to support business decisions through information quality criteria to ensure quality, control, and reliability of information.

5.4   Information is available through standards that foster interoperability, reuse and openness through a trusted open ICT ecosystem.

5.5   Information is protected through a 'privacy and security by design' approach embedded in department culture, processes and systems.

5.6   Information will be managed in an accountable and transparent manner and in compliance with all applicable legislation, regulation, policies, standards, guidelines and best practice information standards.

6 STANDARDS

The department's information quality management principles align to a diverse range of recognised standards, frameworks and information management maturity models. Supporting implementation instruments will be developed with due consideration of these.

---

[1] Information continuum is the whole set of information that represents the relationship between measurement, data, interpretation, explicit knowledge, wisdom and intelligence.

7   POLICY IMPLEMENTATION STRATEGIES

The guiding principles are implemented with strategies that cover the various aspects of information management:

7.1   Information management needs are informed by strategic direction to ensure information is a valued, managed and business-aligned strategic asset, overseen by information governance structures.

7.2   Information will be managed throughout its lifecycle and consider the different approaches required in the different lifecycle stages (discover; specify; collect; display; monitor; archive/destroy).

7.3   Responsibilities and ownership of information and information systems will be defined and assigned, and information assets registered in an appropriate inventory that describes all significant information held by the department, including ownership, access, classification and conditions of use.

7.4   Contemporary information management practices will ensure records (regardless of form or structure), possess the characteristics of authenticity, reliability, integrity and useability and that it is managed in accordance with the *State Records Act 2000*.

7.5   Information will be labelled in accordance with its type and sensitivity, and handled in accordance with its risk-based value and the impact severity of the information being compromised.

7.6   Information will be protected by embedding security and privacy in all stages of the information lifecycle to maintain confidence and trust in the department's ability to hold, handle and use information.

7.7   Intelligence and analytics methods are used to transform information into actionable insights to make informed decisions.

7.8   Responsible information sharing with the public sector, or with authorised third parties, will be through formal sharing agreements that define when and how to safely and effectively share information the department is responsible for.

7.9   Third party arrangements will be assessed using a risk-based approach and consider technical, legal and risk governance. Formal arrangements include ownership, classification, security, privacy, data sovereignty and breach terms and conditions.

7.10   Clear processes will be in place to identify, manage, report and resolve breaches of privacy, including department third party suppliers.

7.11   Employees are aware of and understand information management requirements and staff with specific information management functions adopt effective practices to ensure mature information asset lifecycle management.

8. RESPONSIBILITIES

The following responsibilities apply to information management in the department:

8.1 The Director General is responsible for ensuring the department implements effective information quality management.

8.2 The Chief Information Officer champions the strategic value of information management at an organisational level and is responsible for:

- developing and managing information management standards and architecture across the department to enable quality information;

- driving innovation and capability in information management; and

- leading information governance initiatives for the department.

8.3 Business Service Owners have ultimate responsibility for specific (physical and digital) information assets and ensuring information remains aligned with business objectives, is fit for purpose and maintained at the stated level of quality.

8.4 Information Custodians are responsible for the effective management of specific (physical and digital) information assets throughout the information asset lifecycle, ensuring they are accurate, current, protected, and accessible and shared where applicable.

8.5 Employees are responsible for adhering to this policy.

9. CUSTODIAN

DBCA Chief Information Officer.

10. PUBLICATION

This policy will be made available on the department's intranet.

11. KEY WORDS

Information management; information quality; information asset lifecycle; information sharing; information privacy.

12. REVIEW

This policy will be reviewed no later than September 2027.

13. APPROVAL

Approved by

Mark Webb
DIRECTOR GENERAL
CHIEF EXECUTIVE OFFICER   Date: 15 September 2022