GOVERNMENT OF WESTERN AUSTRALIA

Department of **Biodiversity, Conservation and Attractions**

CORPORATE POLICY STATEMENT NO. 34

INFORMATION BREACH

July 2026

1. OBJECTIVE

To outline the Department of Biodiversity, Conservation and Attractions' (the department's) overarching approach to managing actual or suspected information breaches, as required by the *Privacy and Responsible Information Sharing Act 2024*[1] (PRIS Act).

2. SCOPE

This policy applies to all employees of the department, including the statutory authorities of the Botanic Gardens and Parks Authority, Rottnest Island Authority and Zoological Parks Authority, and any volunteers, contractors or other organisations engaged by the department. It outlines the broad steps the department will take to prevent, identify and report, assess, contain, and mitigate a suspected or actual information breach, including supplier or third-party breaches, to ensure swift action and minimise harm.

3. CONTEXT

An information breach occurs when there is unauthorised access to, or disclosure of information, or if there is a loss of information. Breaches may occur internally, externally or between agencies, affect one or multiple individuals, involve physical or digital information and may involve any type of information that should be protected.

An information breach may be caused by a variety of factors, including:

- Human error, such as sending information to the wrong person, losing a device, or lack of security precautions when working remotely or using mobile devices.
- Insider threats, such as unauthorised access to or misuse of restricted or personal information, including in situations where functions are outsourced by the department.
- Malicious attacks, such as external threat actors compromising networks and exfiltrating information through means such as phishing, malware, or credential theft.
- System failures, such as weak security or misconfiguration of protective controls, or inadequate preventative or detective controls.
- Physical breaches, such as theft of documents or unauthorised access to secure areas.

It is well-recognised that most information breaches involve a human element (e.g. either through direct human error or cyberattacks that rely on human compromise). The department has developed an Information Security Awareness Program to ensure that employees have the skills necessary to identify and avoid cyber security threats and risky behaviours.

[1] The PRIS Act received Royal Assent on 6 December 2024. Parts 1 and 7 and the majority of Parts 2 and 3 are in effect, with the notifiable information breach provisions anticipated to commence on 1 January 2027.

Outside of this program, the department applies and audits access restrictions within the record-keeping system and can identify staff who access information without authorisation. In addition, multiple preventative, protective and detective controls are implemented to protect information including encryption, multifactor authentication, endpoint security, email security, domain security, network security, third party risk assessments and other recommended controls to protect the department from cyberattacks and unauthorised access to its systems.

The impacts and circumstances of any information breach that occurs can vary. As a result, the department will assess and manage such incidents on a case-by-case basis.

4. LEGISLATION

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

Legislation:

- *Biodiversity Conservation Act 2016;*
- *Botanic Gardens and Parks Authority Act 1998;*
- *Conservation and Land Management Act 1984;*
- *Freedom of Information Act 1992;*
- *Information Commissioner Act 2024;*
- *Privacy Act 1988 (Commonwealth);*
- *Privacy and Responsible Information Sharing Act 2024*;
- *Public Sector Management Act 1994;*
- *Rottnest Island Authority Act 1987;*
- *State Records Act 2000;*
- *Swan and Canning Rivers Management Act 2006;* and
- *Zoological Parks Authority Act 2001*.

Policy and strategic frameworks, including any underlying operational procedures:

- Corporate Policy Statement 29 – Privacy of Personal Information;
- the department's Strategic Directions 2025-29;
- Digital Strategy for the Western Australian Government 2021-2025;
- Western Australian Government Cyber Security Policy 2024;
- Western Australian Information Classification Policy;
- Western Australian Open Data Policy; and
- the department's internal information management and security policies, digital IT strategies and enterprise architecture framework for IT.

5. DEFINITIONS / GLOSSARY / ACRONYMS

Information breach	Unauthorised access to, or disclosure of, information or loss of information.
Personal information	Information or an opinion that relates to a person that may directly or indirectly be used to identify that person, including a name, date of birth or address; a unique ID, online ID or username; contact information; location information; technical or behavioural information, identity-related information; and sensitive personal information.

6. POLICY

Preparation and prevention

6.1 The department will conduct regular employee information security awareness training.

6.2 The department will ensure robust security measures are in place, including encryption, multifactor authentication, endpoint security, email security, domain security, network security, third party risk assessments, access controls and regular audits.

Identification and reporting

6.3 The department will implement and maintain effective security identification tools and practices to enable early detection of threats before they pose a risk, including cyber security capabilities and practices to address cyber security risks in accordance with the WA Government Cyber Security Policy.

6.4 Any employee, volunteer, contractor or member of the public who suspects or identifies an information breach must report the incident to privacy@dbca.wa.gov.au.

Assessment, containment, mitigation and notification

6.5 Where an information breach is suspected, detected or reported, the department will take all reasonable steps to immediately contain the breach and mitigate any harm caused.

6.6 The department will conduct an assessment to determine what information was accessed, disclosed or lost during the information breach. The assessment will be undertaken as soon as practicable and will:

- involve staff who are trained and capable of evaluating such incidents and their impact;
- identify the type of information involved (and whether it included personal information) and the number of individuals affected;
- consider whether the access, disclosure or loss of information, may result in serious harm to individuals (particularly if personal information was involved), other organisations or the department.

6.7 The department will prepare a written report of the assessment. The report should consider:

- any weaknesses in information handling that may have contributed to the breach;
- the effectiveness of the department's response to the breach (including the effectiveness of this policy);
- any corrective actions required to prevent future breaches and mitigate potential harm;
- which, if any, individuals, agencies or other bodies need to be notified (e.g. individuals whose personal information has been compromised, Information Commissioner, WA Police Force, insurance agencies, etc.).

6.8 All information relevant to the assessment, containment, mitigation and notification of an information breach will be stored securely and managed in accordance with Corporate Policy Statement No. 7: Information Quality Management, Operational Procedure: Information Quality Management Framework, Corporate Policy Statement No. 70: Information Security Management; and the department's Recordkeeping Plans.

Managing supplier or third-party information breaches

6.9 In the event that an information breach occurs with regard to an external service provider, external government agency, or any other third party that the department has shared information with, it shall be managed in accordance with this policy and in coordination with the contract manager or relevant department contact.

7. STANDARDS

The following documents provide direction and standards, including expectations regarding employee behaviour in relation to this policy:

- PRIS Act;
- WA Government PRIS Readiness Plan and supporting Readiness Guidance documents (including the Readiness Checklist); and
- The department's Code of Conduct.

8. POLICY IMPLEMENTATION STRATEGIES

The department will:

8.1 Develop and maintain an Information Breach Response Plan.

8.2 Develop and maintain an Information Breach Register.

8.3 Identify and develop suitable training and awareness activities.

8.4 Ensure that any Shared Information Agreements have suitable arrangements for managing an information breach.

8.5 Ensure that contracts or agreements with service providers, external government agencies, or other third parties have suitable arrangements for managing an information breach.

9. CUSTODIAN

Deputy Director General Science, Strategy and Governance.

10. PUBLICATION

This policy will be made available on the department's intranet and website and must be provided to any person on request.

11. KEY WORDS

Information breach, personal information, privacy, assessment, containment, mitigation, notification, PRIS.

12. REVIEW

This policy will be reviewed when the full provisions of the PRIS Act commence in 2027.

13. APPROVAL

Approved by

Stuart Smith
DIRECTOR GENERAL
CHIEF EXECUTIVE OFFICER Date: 31 July 2026