Policy Number: 120

Banana Shire Council
Adopted: 26 September 2023

DATA BREACH RESPONSE POLICY

SCOPE

This policy outlines Council's approach to dealing with an identified breach in the maintenance, integrity, security, privacy, and confidentiality of data it is entrusted to store and maintain in order to conduct Council business.

LEGISLATION

Local Government Act 2009
Information Privacy Act 2009
Right to Information Act 2009

OBJECTIVE

To ensure that Council responds to any actual or threatened breach of data security by a person or persons unknown, in the most effective manner with a focus on minimizing the risk of serious harm to affected individuals immediately and in the future.

DEFINITIONS

CEO	Chief Executive Officer A person who holds an appointment under section 194 of the Local Government Act (2009). This includes a person acting in this position
Council	Banana Shire Council
Council Employee	Local Government Employee (a) The CEO, or (b) A person holding an appointment under section 194 of the Local Government Act (2009).
Data Breach	A data breach occurs when personal information that an entity holds is subject to unauthorized access or disclosure or is lost. In example: 1. Human error – personal information stored on a USB drive is lost or misplaced. 2. Mistakenly disclosed – personal information forwarded in an email to unintended recipients. 3. Deliberate Act – Council's cyber-security safe-guards are purposely penetrated with malicious intent and/or for criminal gain. Attempted Breach – an unsuccessful attempt to gain unauthorised access.

Data Breach Response Plan	Council's action plan in the event of a data breach or attempted breach, including escalation criteria, individual employee and Response Team responsibilities, risk assessment criteria and risk mitigation strategies.
Data Breach Response Team	A clearly identified and readily contactable group with specific accountabilities, convened at the time a breach is detected, and charged with ensuring Council's most effective response.
Mandatory Data Breach Notification	Information provided to the Office of the Information Commissioner (Old) in the event of a breach. Provision of the report is NOT mandatory at the time of writing.

POLICY

Council takes all reasonable steps to ensure that personal information is collected, stored and utilised securely and only for the purpose for which it was collected.

Banana Shire Council will comply with the Information Privacy Principles set out in Schedule 3 of the *Information Privacy Act 2009.*

Responding to a Privacy Breach

Council will follow the following steps on responding to a privacy breach:

1. Control the breach
2. Evaluate the risk of serious harm
3. Consider notifying affected individuals and Office of the Information Commissioner
4. Prevent a repeat

Council will maintain a detailed Data Breach Response Plan incorporating immediate escalation to a prescribed level of decision-making once a breach is detected, assessment of the extent, nature and likelihood of any potential harm to affected individuals, and identification of the most effective remediation action. The Data Breach Response Plan will also incorporate a breach/risk assessment criteria, recording, reporting, and compliance requirements and a perpetual 'response effectiveness' review process.

In addition to internal management of data breaches Council will undertake notifications to the Office of the Information Commissioner or other mandatory reporting requirements such as the Queensland Government Enterprise Architecture of the Commonwealth Notifiable Data Breaches Scheme.

PROCEDURE

Procedures as approved and issued by the Chief Executive Officer, and subject to further revision, amendment and issue under the authority of the Chief Executive Officer.

CERTIFICATION

.....

CHIEF EXECUTIVE OFFICER
BANANA SHIRE COUNCIL

28/9/2023

DATE