Blackall-Tambo Regional Council

# Data Breach Response Plan

| | |
|---|---|
| Policy Number: P29 | Effective Date: 15.04.2026 |
| Version Number: Two | Review Date: 15.04.2030 |
| Policy Compiled by: Information Technology Officer | |
| Policy Approved by: Chief Executive Officer | |

## PURPOSE AND SCOPE

This data breach response plan (response plan) sets out procedures and clear lines of authority for Blackall-Tambo Regional Council (BTRC) staff in the event that the BTRC experiences a data breach (or suspects that a data breach has occurred).

A data breach covered by the Information Privacy Act 2009 (QLD) (IP Act) occurs when personal information is lost or subjected to unauthorised access or disclosure. For good privacy practice purposes, this response plan also covers any instances of unauthorised use, modification or interference with personal information held by the BTRC. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information, and give rise to a range of actual or potential harms to individuals and entities.

This response plan is intended to enable the BTRC to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the IP Act scheme. Our actions in the first 24 hours after discovering a data breach are crucial to the success of our response.

The plan sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist the BTRC to respond to a data breach.

This response plan should be read in conjunction with the BTRC Data Breach Policy.

Protection of our information and data is paramount. This response plan will provide a checklist for responding to a security incident or potential data breach. An incident can be intentional or unintentional, and this response plan could be implemented in response to many events having an adverse effect on the Council Network.

## APPLICABILITY

This response plan process applies to all employees, administrative consultants, contractors, temporary personnel, and the like who may experience or witness a security incident or possible data breach. After discovery, this process provides IT with a checklist or outline for responding so that steps or information

related to the incident are not missed. The Council is committed to protecting our information and responding appropriately to a security incident or data breach.

## GUIDELINES

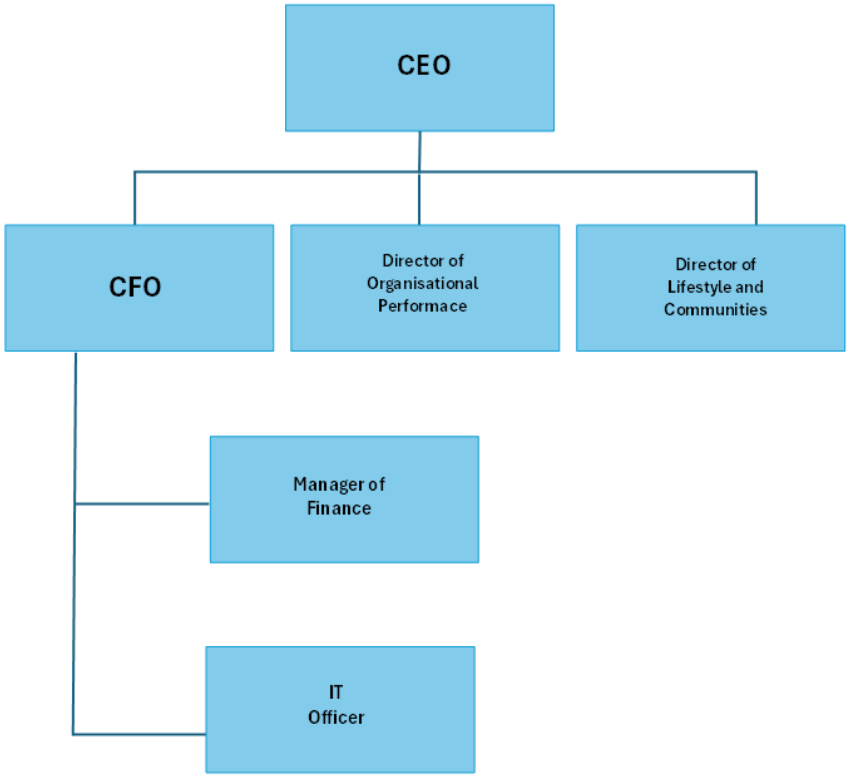
This response plan describes our safeguards to protect sensitive information, including Personally Identifiable Information (PII). These safeguards are provided to:

a) Protect the confidentiality, integrity and availability of data and the Council Network;
b) Protect against a data breach that could result in harm or inconvenience to a client or user and meet any notification requirements;
c) Protect against anticipated threats or hazards to the security or integrity of sensitive information, including PII;
d) Identify and assess the risks that may threaten PII;
e) Conduct a reasonable investigation to determine the likelihood of information that has been or will be misused;
f) Conduct a post-incident investigation to capture lessons learned;
g) Develop written policies and procedures to manage and control these identified risks or vulnerabilities;
h) Adjust the Information Security Program to reflect changes in technology, the sensitivity of data stored, and internal or external threats to information security.

The response plan will be tested annually to ensure all participants on the Incident Response Team (IRT) know their roles in the event of a true incident.

## ROLES & RESPONSIBILITIES

Incident Response Team (IRT)




## PROCESS

This section establishes suggested steps for responding to an incident and initiating the response plan. Each incident will present unique issues that will require resolution by the IRT.

## PREPARATION

1. Ensure appropriate policies, procedures and systems are in place to identify data breaches and report them appropriately.
2. Ensuring policies and procedures are in place for responding to data breaches, including how to undertake date breach assessment with appropriate risk assessment, notification, and interconnected policies and procedures such as an agency cyber incident response plan, information security policy, notification and communication procedures.
3. Identifying specific reporting lines, internal bodies decision-makers and escalation points attached to controls and other mechanisms used to identify data breaches and respond to data breaches. This should include the key reporting roles and responsibilities in a data breach response and identify and any specific internal committee or body, such as a Data Breach Response Team, to be established as part of the data breach response process.
4. Identifying specific roles and positions, including those making up the Data Breach Response Team, and how these may vary depending on the type or severity of a data breach. Depending on the type of breach, this Team may include representatives from the Council's IT, cybersecurity, communications, HR, Legal, Senior Executive and Privacy teams. Subject matter experts may also need to be stood up depending on the source and nature of the data breach. Each member should be allocated responsibilities (e.g. making escalation decisions, reporting obligations, maintaining,

testing and updated the Data Breach Policy, data breach recordkeeping, and post data breach review and evaluation.
5. Ensuring there is a broad awareness across the Council of the policies, procedures and obligations in place.

## IDENTIFICAITON

1. Anyone suspecting or noting a security incident, data breach or potential system compromise, or malicious activity contacts Information Security, the IRT or outside incident responder on the team [All referred to as "Information Security" in this document]
2. Determine if there has been a security incident, and the nature and seriousness of the incident, by considering the following questions and discussing them with Information Security, and document initial triage.
    - Does the system contain Council Sensitive Information or PII?
    - Is there a chance outside law enforcement may need to get involved?
    - Is there a requirement or desire to perform a forensics analysis of the system compromise?
    - If the answer is "yes" to any of these questions then immediately coordinate actions to be taken with IT and the Executive Leadership Team (ELT), and apply the below as appropriate.
    - If the answer is "no" to all the questions, then apply the below as appropriate.
    - Do preliminary analysis - isolate the compromised system by disconnecting the network cable. If this is not feasible or desirable, Information Security can block access to the compromised system via the network.
3. Determine the security incident type - try to determine the cause of the malicious activity and the level of system privilege attained by the intruder and implement appropriate remedial measures.

## CONTAINMENT & MITIGATION

If a system is compromised:

- Disable any compromised accounts and terminate all processes owned by them.
- Compile a list of IP addresses involved in the incident, including log entries if possible, and forward the data to Information Security.
- Determine the users that need to change their passwords due to the compromise, as well as whether they have accounts on other systems using the same credentials and notify the IT administrators for those systems.
- Backup the local password file, if appropriate, so you can compare who has and who has not changed their passwords after notification.
- Notify Information Security if your system uses Lightweight Directory Access Protocol (LDAP) authentication to authenticate users.
- Notify the owners of the compromised accounts and reissue credentials. Consider the likelihood of the intruder having access to the compromised account email and utilize other contact methodology.
- Determine whether all affected users have established new user IDs and passwords.
- Rebuild the system and verify that its network access should be re-established by contacting Information Security.
- Information Security should perform a network vulnerability scan of the system after it is unblocked to identify any unresolved security issues that might be used in future attacks against the system.

## ASSESSMENT

The IP Act imposes specific obligations for certain types of data breaches. It is therefore necessary to assess a data breach against the criteria prescribed under the IP Act to determine if the data breach is an Eligible Data Breach.

## NOTIFICATION

1. If a security incident is suspected to be a data privacy breach, immediately notify the IRT, including the ELT.
2. Determine what information was suspected to be breached, i.e., specific individuals' first and last names with a type of PII.
3. When appropriate, bring in an incident response expert or law enforcement to investigate. Identify the scope, time frame and source(s) of breach, type of breach, whether data encryption was used and for what, possible suspects (internal or external, authorized or unauthorized, employee or non-employee user).
4. Review for other compromised systems.
5. Monitor all systems for potential intrusions.
6. Determine the notification requirements (statutory or contractual) and address within the required timeframe.

## POST-INCIDENT LESSONS LEARNED

1. Hold a meeting of the IRT within 48 hours of completion of response.
2. Review chronology of the event.
3. Identify what went wrong and what went right. For instance, "encryption was used on the file server containing Council Confidential Information and PII."
4. Identify the threat or vulnerabilities that were exploited and determine whether it/they can be alleviated.
5. Review if all intrusion detection or prevention was in place, active and up to date.
6. Document "lessons learned" and assign appropriate updates to Information Security Program.

## COMPLIANCE

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. Where necessary, obligations to external authorities will be met.

## ACCOUNTABILITY

All users are accountable for reporting any suspected data breach of the Council Network to the IT Department.

Internal Audit is responsible for ensuring compliance with the Council Information Security Policy and the controls created to safeguard the Council Network.

IT responds to the incident, and analyses and collects the audit records and any logs and redeploys new credentials to affected users after identification.

IT is responsible for maintaining updates to the Information Security Program post incident and at a minimum annually.

The Incident Response Team is responsible for documenting the types of personal information that may have been breached, provides guidance throughout the investigation on privacy issues, and assists in developing the communication plan to impacted individuals.

## EXCEPTIONS

Any exceptions must be approved by the IT Department and ELT.

## POLICY REVIEW

This policy will be reviewed when any of the following occur:

a) As required by legislation

b) Other circumstances as determined by the Chief Executive Officer

Notwithstanding the above, this policy is to be reviewed at intervals of no more than four (4) years.

## VERSION CONTROL

| | |
|---|---|
| Version 1 | New Document 21-04-21 |
| Version 2 | Updated 15-04-2026 |
| | |

## RECORDS

When completed and approved, the original signed hard copy of the policy is filed in the Master File. Electronic copies are saved in the appropriately labelled folder in Magiq.