Blackall-Tambo Regional Council

Incident Response Plan

Policy Number: P30	Effective Date: 21.04.2021
Version Number: One	Review Date: 21.04.2025
Policy Compiled by: Information Technology Officer	
Policy Approved by: Chief Executive Officer	

PURPOSE OF THE POLICY

The purpose of this Incident Response Plan ("IRP") is to provide guidance on the appropriate steps to be taken and documented in the event of a possible security incident or data breach, from the time of suspected breach to post-incident response closure, so that all incidents are handled in a consistent manner and the exposure to the potentially breached party is limited. It also provides a methodology for collecting evidence in the event of criminal activity. Documentation of responsive actions taken in connection with any security incident or data breach, as well as documentation of the post-incident events and actions taken, is critical in making appropriate changes to business practices to improve the safeguarding and handling of Council Sensitive Information and Personally Identifiable Information (PII) (as with all privacy and security policies, protected information sets must be defined consistently throughout the organization).

APPLICABILITY

This IRP 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.

SCOPE

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

GUIDELINES

This IRP describes our safeguards to protect sensitive information, including 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 IRP will be tested annually to ensure all participants on the Incident Response Team (IRT) know their roles in the event of a true incident.

PROCESS

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

INCIDENT RESPONSE PROCESS – INITIAL DISCOVERY

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 Director of Finance, Corporate and Community Services, 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.
4. 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 or not 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 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.

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.

INCIDENT RESPONSE – BREACH NOTIFICATION

1. If a security incident is suspected to be a data privacy breach, immediately notify the IRT, including the Director of Finance, Corporate and Community Services and the Chief Executive Officer.
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 conduct an investigation. 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.

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. We reserve the right to advise appropriate authorities of any violation of law.

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 Senior Management.

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

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.