Data Breach & Incident Response Procedure

Business: MarketingSteve
ABN: 52719351544
Effective Date: October-2026
Last Reviewed: October-2026
Review Frequency: Annually and following a material incident

1. Purpose

This procedure establishes the steps MarketingSteve will take to identify, contain, assess and respond to suspected or confirmed data breaches and information security incidents.

The objective is to minimise harm to clients, individuals and the business while complying with applicable legal and contractual obligations.

2. Scope

This procedure applies to incidents involving:

- Business or client information.
- Personal or confidential information.
- Business-owned devices and cloud accounts.
- Client systems accessed by the consultant.
- Authorised subcontractors and relevant third-party service providers.

It applies regardless of whether the incident results from human error, technical failure, malicious activity or other circumstances.

3. What Constitutes an Incident?

A security incident may include:

- Loss or theft of a device containing business or client information.
- Unauthorised access to an account, system or file.
- Accidental disclosure of confidential information to an unintended recipient.
- Phishing, credential theft, malware or ransomware.

- Loss, alteration or corruption of important data.
- Unauthorised sharing or exposure of personal information.
- Compromise of a client platform or third-party service.
- Accidental submission of confidential or personal information to an unauthorised external service, including an AI platform.

Not every security incident constitutes a legally notifiable data breach. Each incident must be assessed according to its circumstances and applicable obligations.

4. Responsibility

The sole trader is responsible for coordinating the response to incidents affecting business-controlled information, systems or activities.

Where an incident involves client-owned systems or information, the consultant will cooperate with the relevant client and its authorised representatives.

External IT, legal, insurance or cybersecurity assistance may be obtained where reasonably necessary.

5. Step One – Identify and Contain

Upon becoming aware of a suspected incident, the consultant must take reasonable steps to prevent further unauthorised access, disclosure or loss.

Depending on the circumstances, actions may include:

- Securing affected devices or accounts.
- Changing compromised passwords.
- Revoking exposed credentials, tokens or access permissions.
- Disconnecting affected devices where appropriate.
- Suspending unauthorised data transfers or sharing links.
- Contacting a relevant platform or service provider.
- Requesting deletion or secure return of information sent to an unintended recipient.
- Seeking specialist technical assistance.

Immediate containment should be prioritised, while taking reasonable steps to preserve evidence needed to investigate the incident.

6. Step Two – Assess the Incident

The consultant must assess the nature, scope and potential consequences of the incident as promptly as reasonably practicable.

The assessment should establish:

1. What happened and when it was discovered.
2. Which systems, accounts or information were affected.
3. Whether personal or confidential information was involved.
4. Whether information was accessed, lost, altered or disclosed without authorisation.
5. Which clients, individuals or other parties may be affected.
6. Whether the incident remains ongoing.
7. What harm may reasonably result.
8. What further containment, recovery or notification measures are necessary.

Where circumstances are unclear, the incident should be treated cautiously until sufficient information is available.

Incidents involving sensitive information, identity documents, financial credentials, substantial personal information or ongoing unauthorised access should receive heightened priority.

7. Step Three – Notify Relevant Parties

7.1 Client notification

Where an incident is known or reasonably suspected to materially affect a client's information or systems in connection with the Services, the consultant will notify the affected client without undue delay.

Where reasonably practicable, initial notification should occur within 48 hours of becoming aware of the incident, consistent with the Standard Service Agreement.

The initial notification should explain what is known, the immediate steps taken and any assistance or action reasonably required.

The consultant may provide further updates as additional information becomes available.

7.2 Legal and regulatory notification

The consultant will determine whether any legal notification obligation applies, taking appropriate professional advice where necessary.

Where the business is subject to the Australian Notifiable Data Breaches scheme, a suspected eligible breach must be assessed in accordance with the statutory requirements.

Where an eligible breach is established and notification is required, the relevant individuals and the Office of the Australian Information Commissioner must be notified as soon as practicable, subject to applicable exceptions.

Other legal, regulatory or contractual reporting obligations must also be considered where relevant.

7.3 Client-managed information

Where an incident concerns information controlled by a client, the consultant will provide reasonable assistance to support the client's investigation and notification responsibilities.

The consultant will not ordinarily issue regulatory or public notifications on behalf of a client without authorisation, except where independently required by law.

8. Step Four – Recover and Remediate

Once the incident has been contained and assessed, reasonable steps will be taken to restore secure operations and reduce the likelihood of recurrence.

These may include:

- Restoring files or system access.
- Applying security updates.
- Strengthening authentication requirements.
- Removing unauthorised access permissions.
- Revising data handling practices.
- Seeking corrective action from relevant service providers.
- Updating affected clients on remediation measures.

Recovery activities should be proportionate to the incident and the business's responsibilities.

9. Incident Documentation

A reasonable written record must be maintained for material incidents.

The record should include:

- Date and time of discovery.
- Description of the incident.
- Systems and information affected.
- Assessment of actual or potential harm.

- Containment and recovery steps taken.
- Parties notified and relevant correspondence.
- Any legal or professional advice obtained.
- Corrective actions and the date of closure.

Documentation must be stored securely and retained in accordance with applicable legal and business requirements.

10. External Communications

Communications concerning a significant incident must be accurate, factual and appropriately limited to information reasonably established at the time.

The consultant should avoid speculation, premature conclusions or statements that may interfere with an ongoing investigation.

Where appropriate, legal or specialist advice should be obtained before making significant public or regulatory statements.

Nothing in this section permits withholding, delaying or misrepresenting information where disclosure is required by law or contract.

11. Post-Incident Review

Following a material incident, the consultant will review:

- The underlying cause.
- Whether the response was timely and effective.
- Whether existing safeguards were adequate.
- Whether additional security measures are reasonably necessary.
- Whether relevant business policies or procedures require updating.

The purpose of the review is to strengthen business practices and reduce the likelihood or impact of future incidents.

12. Ongoing Readiness

The business will maintain reasonable incident response readiness through current security practices, access to relevant accounts and providers, and periodic review of this procedure.

The procedure will be reviewed annually and following material incidents or relevant legal changes.