Spatial Media Data Breach Response Plan

V2.07 — 15 JANUARY 2024

Table of Contents

1.0 Scope

This data breach response plan (response plan) sets out procedures and clear lines of authority for Spatial Media (SM) staff in the event that Spatial Media, or information SM collects and holds on behalf of a client or third-party stakeholder either acting as Spatial Media or through associated products owned by Spatial Media (e.g. Community Analytics, Spatial Engage), experiences a data breach (or suspects that a data breach has occurred).

The guidelines within this document can also apply to incidents which interrupt service delivery but do not involve a data breach.

1.1 Internal roles and responsibilities

- The following RACI matrix outlines who is Responsible, Accountable, Consulted and Informed for various security-related matters, where
    - RACI stands for:
        - Responsible – the role is directly responsible for delivering the solution in the scenario
        - Accountable – the role is held accountable for ensuring the solution in the scenario is satisfactorily delivered
        - Consulted – the role is consulted for their opinion on the solution in the scenario
        - Informed – the role is kept informed of updates or changes to the solution in the scenario
    - Roles are defined as:
        - Directors – the board of directors or persons acting in Director-level roles
        - CTO – the Chief Technical Officer
        - Team lead – usually the dev lead, but can also be the lead manager of a department or team where the scenario applies
        - PMs – the project manager responsible for the project where the scenario applies

- Staff – the staff, typically other developers but can extend to all staff including contractors, who are involved in the project where the scenario applies
- Client – the external client-side point of contact for the project where the scenario applies

Scenario	Directors	CTO	Team lead	PMs	Staff	Client
Minor security issues	C, I	R, A, C	R, A	A	R, A	I
Major security issues	A, C, I	R, A, C	R, A	A	R, A	I
Up-time and performance	I	R, A, C	R, A	I	R	I
Data breach response	A, C, I	R, A, C	R, A	A	R, A	I
Phishing protection	R, A	A, C	A	I	I	N/A
Data encryption and protection	R, A	R, A	C	I	I	N/A
Secure deletion	C	R, A	C	R, A	I	N/A
Legal and compliance	R, A	C	C	I	N/A	I
Business continuity and disaster recovery	R, A	C	C	C	C	N/A

2.0 Overview

A data breach occurs when sensitive information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused or exacerbated by a variety of factors, affect different types of information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

This response plan is intended to enable Spatial Media to contain, assess and respond rapidly to data breaches in an effective manner, and to help mitigate potential harm to affected individuals. It sets out the responsibilities of related and appropriate staff in the event of a data breach, clarifies the steps they should follow, and documents processes to assist Spatial Media in responding to a data breach.

2.1 Overarching response flow

1. **Detect**
    a. Data breach or incident is discovered by an SM staff member, or SM is otherwise alerted
2. **Report**
    a. Staff should immediately notify the Team Lead, the Project Manager and the CTO of the suspected data breach.
    b. Record and advise of the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and the context of the affected information and the breach.
3. **Assess**
    a. The CTO, Team Lead and appropriate Project Manager should work together to determine whether a data breach has or may have occurred.
    b. Determine whether the data breach is serious enough to escalate to Directors
    c. If so, immediately escalate to Directors.
4. **Resolve & Notify**

a. CTO (Benoit St-André) convenes the Incident Response Team and relevant internal stakeholders:
    i. Managing Director: Jai Eakin
    ii. Spatial Tech Director: Morley Foster
    iii. Spatial Media Canada Director: Aaron Bernard
    iv. Creative/Web Director: Nathan Green
    v. Head of Client Engagement: Dan Cain
    vi. Legal and records: Morley Foster
    vii. Technical lead: Loïc Bisiere
b. CTO works to resolve the issue by resolving the attack point as the number one priority, isolating its impact wherever possible
c. Then work further to understand if additional attack points are exposed, and the extent of the data breach
d. Notification is also part of this step
e. For more detail on this step, see *4.0 Detailed resolution workflow*

3.0 Escalation

3.1 Assessment and escalation discretion

- The CTO (and Team Leads where appropriate) may use their discretion in deciding whether to escalate to directors and broader Incident Response Team (response team).
- Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Incident Response Team (response team).
- For example, an SM employee may, as a result of human error, send an email containing information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the offender can contact the recipient and the recipient agrees to delete the email, it may be that there is no advantage in escalating the issue to the response team.
- The CTO (and Team Leads) should use their discretion in determining whether a data breach or suspected data breach requires escalation to the response team.
- In making that determination, Technical Directors should consider the following questions:
    - Are multiple entities affected by the breach or suspected breach?
    - Is there (or may there be) a real risk of serious harm to the affected entities?
    - Does the breach or suspected breach indicate a systemic problem in Spatial Media's processes or procedures?
    - Could there be media or stakeholder attention as a result of the breach or suspected breach?
- **If the answer to any of these questions is 'YES', then it may be appropriate for the CTO to notify the response team.**

3.2 Responsibility to notify

- If the CTO decides not to escalate a minor data breach or suspected data breach to the response team for further action, they should:

- send a brief email to the Board of Directors and to the appropriate Team Lead that contains the following information:
    - description of the breach or suspected breach
    - action taken by the Technical Director or SM staffer to address the breach or suspected breach
    - the outcome of that action, and
    - the Technical Director's view on what further action may be required
- save of copy of that email in the following cloud-based archive:
    - Data Breach Response – reports and investigation of data breaches within Spatial Media (internal link)

- For major data breaches, CTOs should work with the response team to determine the appropriate parties to notify, and make those notifications within a timely manner

4.0 Detailed resolution workflow

3.1 Process

- There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.
- There are four key steps to consider when responding to a breach or suspected breach:
    - **STEP 1:** Contain the breach and do a preliminary assessment
    - **STEP 2:** Evaluate the risks associated with the breach
    - **STEP 3:** Notification
    - **STEP 4:** Prevent future breaches
- The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.
- The response team should refer to the technical guides relating to the area and type of data breach, to handle and assess the information security breaches which provides further detail on each step.
- Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.
- In reconsidering Spatial Media's processes and procedures to reduce the risk of future breaches (Step 4), the response team should also refer to Spatial Media's policies on securing personal and client information. This guide presents a set of non-exhaustive steps and strategies that may be reasonable for Spatial Media to take in order to secure sensitive information, and considers actions that may be appropriate to help prevent further breaches following an investigation.
- The following checklist is intended to guide the response team in the event of a data breach, and alert the response team to a range of considerations when responding to a data breach.

4.2 Step-by-step

4.2.1 Step 1 – Contain the breach and make a preliminary assessment

- Convene a meeting of the data breach response team.
- Immediately contain breach:
    - IT to implement a data and connectivity lockdown if necessary.
    - Relevant security and law enforcement to be alerted if necessary. (Especially in the case of lost property containing data)
- Inform the relevant SM Project Manager in order for them to notify the effected stakeholders to communicate updates and progress.
- Ensure evidence is preserved to determine the cause of the breach, allowing Spatial Media to take appropriate corrective action.
- Consider developing a communications or media strategy to manage public expectations and media interest.

4.2.2 Step 2 – Evaluate the risks for individuals associated with the breach

- Conduct initial investigation, and collect information about the breach promptly, including:
    - the date, time, duration, and location of the breach
    - the type of personal information involved in the breach
    - how the breach was discovered and by whom
    - the cause and extent of the breach
    - a list of the affected stakeholders, or possible affected stakeholders
    - the risk of serious harm to the affected stakeholders
    - the risk of other harms.
- Determine whether the context of the information is important.
- Establish the cause and extent of the breach.
- Assess priorities and risks based on what is known.
- Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made.

4.2.3 Step 3 – Make the appropriate notifications

- Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
- Determine whether to notify affected stakeholders – is there a real risk of serious harm to the affected entities? In some cases, it may be appropriate to notify individuals immediately; e.g., where there is a high level of risk of serious harm to affected stakeholders.
- For major data breaches involving PII, inform the relevant federal authorities:
    - In Australia: **Office of the Australian Information Commissioner (OAIC)**:
        - Under the Notifiable Data Breaches (NDB) scheme, you must notify the OAIC if there is a data breach that is likely to result in serious harm to any individuals whose personal information is involved in the breach.
        - Notifications should include details of the breach, the kind of information affected, and recommendations about the steps individuals should take in response to the breach.
    - In Canada: **Office of the Privacy Commissioner of Canada (OPC)**:
        - Under the Personal Information Protection and Electronic Documents Act (PIPEDA), you must report to the OPC any breach of security safeguards involving personal information under your control if it is reasonable to believe that the breach creates a real risk of significant harm to individuals.
        - The report should include details about the circumstances of the breach, the personal information involved, and the steps taken to mitigate the breach and notify affected individuals.
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where SM is contractually required or required under the terms of a Confidentiality Agreement or similar obligation to notify specific parties.

4.2.4 Step 4 – Review and take action to prevent future breaches

- Fully investigate the cause of the breach, and provide a detailed **Post-Incident Review** to evaluate the response and identify lessons learned.
- Report to Spatial Media Executives on outcomes and recommendations:
    - Update security and response plan, policies and procedures if necessary.
    - Revise staff training practices if necessary.
- Notify other parties of this review where appropriate.
- Take pre-emptive measures to stop future similar breaches, including modifying staff training, adjusting automatic scanning policies, or reviewing access controls

5.0 Mitigating the consequences of a breach

- Where appropriate, Spatial Media should work with impacted clients and stakeholders to mitigate the consequences of a breach. These steps include:

5.1 Immediate Incident Response

- **Incident Response Team Activation**: Establish and activate a dedicated incident response team (IRT) that includes key personnel from IT, legal, communications, and management to handle the breach.
- **Initial Assessment**: Conduct an immediate assessment to understand the scope and impact of the breach, including identifying the data involved and the potential risks.

5.2 Containment Measures

- **Isolation**: Isolate affected systems to prevent further data loss or unauthorised access.
- **Patch Vulnerabilities**: Identify and patch any vulnerabilities that were exploited during the breach.

5.3 Communication and Notification

- **Internal Communication**: Inform relevant internal stakeholders about the breach, including senior management and affected departments.
- **Client Notification**: Notify clients promptly with detailed information about the breach, including the nature of the breach, the data affected, and the steps being taken to address it.
- **Regulatory Notification**: Notify appropriate regulatory bodies as required by law.

5.4 Support for Affected Individuals

- **Guidance and Recommendations**: Provide affected individuals (including client employees or customers) with guidance on steps they can take to

protect themselves, such as changing passwords, monitoring accounts, and being aware of phishing attempts.

- **Helpline and Support**: Set up a dedicated helpline or support channel to assist affected individuals with any concerns or questions.

5.5 Investigation and Analysis

- **Root Cause Analysis**: Conduct a thorough investigation to determine the root cause of the breach and document findings.
- **Forensic Analysis**: Where required, engage cybersecurity experts to perform forensic analysis to understand how the breach occurred and to gather evidence.

5.6 Remediation and Recovery

- **Data Restoration**: Work on restoring any lost or compromised data from backups.
- **System Restoration**: Ensure that affected systems are securely restored and verified before being brought back online.
- **Ongoing Monitoring**: Implement enhanced monitoring of systems to detect any further suspicious activity.

5.7 Review and Reporting

- **Post-Incident Review**: Conduct a post-incident review to evaluate the response and identify lessons learned.
- **Report to clients**: Provide clients with a detailed report on the breach, including the cause, the response actions taken, and any measures implemented to prevent future breaches.

5.8 Preventive Measures

- **Policy Updates**: Update security policies and procedures based on lessons learned from the breach.

- **Training and Awareness**: Provide additional training for staff on security best practices and how to recognize and respond to potential security threats.
- **Regular Audits**: Conduct regular security audits and vulnerability assessments to identify and mitigate potential risks.

6.0 Changes to this policy

- This policy is reviewed annually and all staff will be notified of changes or reminded of the key aspects of this policy each year
- Changes to this policy will be peer reviewed prior to being committed into the policy

7.0 Contact Information

For questions or concerns related to this policy, please contact:

- Benoit St-André — Chief Technical Officer
  - benoit@spatialengage.io
- Jai Eakin — Managing Director
  - jai@spatialmedia.io