Spatial Media
Data Breach Response Plan

Last Updated: 2 November 2018

Spatial Media
T: 1300 772 842
3 Bonython Street, Windsor QLD 4030
ABN: 90 169 634 431

SPATIALMEDIA
VIRTUALLY DIFFERENT

Data breach response plan

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,experiences a data breach (or suspects that a data breach has occurred).

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 Spacial Media in responding to a data breach.

DATA BREACH OCCURS/DATA BREACH SUSPECTED

Discovered by SM staff member, or SM otherwise alerted

What should the Spatial Media staff member do?

- Immediately notify the Technical Director of the suspected data breach.
- Record and advise your Technical Director 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.

What should the Technical Director do?

- Determine whether a data breach has or may have occurred.
- Determine whether the data breach is serious enough to escalate to the Data Breach Response Team (some breaches may be able to be dealt with at the Technical Director level).
- If so, immediately escalate to the Data Breach Response Team.

ALERT SM DATA BREACH RESPONSE TEAM COORDINATOR

- Coordinator convenes response team, or relevant internal stakeholders:

Legal & Records	IT	Corp. & Comms.	Strat. & Regulation
Morley Foster	Tim Sheehan	Jared Adamo	Aaron Bernard

Escalation

When should Directors escalate a data breach to the SM Data Breach Response Team?

Technical Directors to use discretion in deciding whether to escalate to the response team

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach 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.

Technical Directors 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 Technical Director to notify the response team.

Directors to inform the response team Coordinator of minor breaches

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

- **send a brief email to the response team Coordinator (relating to the area(s) of business) 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)

SM Data Breach Response Team checklist

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.

Records management

Documents created by the response team should be saved in the following Box Folder:

- Data Breach Response – reports and investigation of data breaches within Spatial Media (http://bit.ly/CA-SM-DRM)

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.
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.
STEP 3 Consider breach notification		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.
		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.
STEP 4 Review and take action to prevent future breaches		Fully investigate the cause of the breach.
		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.

Contact for More Information

Nathan Green
Technical Director
nathan@spatialmedia.com.au
0423 490 622

Aaron Bernard
Creative Director
aaron@spatialmedia.com.au
0431 332 882

SPATIALMEDIA
VIRTUALLY | DIFFERENT