Data Security Breach Incident Management Policy

Contents

1. Aim

The aim of this policy is to standardise Spectrum Analysis' response to any reported data breach incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents it aims to ensure that:

- incidents are reported in a timely manner and can be properly investigated
- incidents are handled by appropriately authorised and skilled personnel
- appropriate levels of management are involved in response management
- incidents are recorded and documented
- the impact of the incidents are understood and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and procedures.

2. Definition

A data security breach is considered to be "any loss of, or unauthorised access to, Spectrum Analysis or any customer's data".

Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential Data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit

For the purposes of this policy data security breaches include both confirmed and suspected incidents.

3. Scope

This policy applies to all Spectrum Analysis or any customer's data, regardless of format, and is applicable to all staff, contractors and data processors acting on behalf of Spectrum Analysis. It is to be read in conjunction with Spectrum Analysis' Information Security Policy.

4. Responsibilities

4.1 Information users

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage. Any suspected breaches are to be personally reported to the Managing Director of Spectrum Analysis.

5. Data Classification

Data security breaches may vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that Spectrum Analysis is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

Any reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following Data Categories:

5.1 Public Data:
Information intended for public use, or information which can be made public without any negative impact for Spectrum Analysis'.

5.2 Internal Data:
Information regarding the day-to-day business and operations of Spectrum Analysis'. Primarily for staff use, though some information may be useful to third parties who work with Spectrum Analysis'.

5.3 Confidential Data:
Information of a more sensitive nature for the business operations of Spectrum Analysis and our clients, representing basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role within Spectrum Analysis'.

5.4 Highly confidential Data:
Information that, if released, will cause significant damage to Spectrum Analysis' business activities or reputation, or would lead to breach of the Data Protection Act. Access to this information should be highly restricted.

6. Data Security Breach Reporting

Confirmed or suspected data security breaches should be reported promptly. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting process. See **Appendix 1**.

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the lead responsible officer to lead should be. See **Appendix 2**.

All data security breaches will be centrally logged to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

7. Data Breach Management Plan

The management response to any reported data security breach will involve the following four elements. See **Appendix 3** for suggested checklist.

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist for Data Security

Breaches. An activity log recording the timeline of the incident management should also be completed. See **Appendix 4**.

8. Authority

Staff, contractors, and consultants who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

9. Review

The Managing Director will monitor the effectiveness of this policy and carry out regular reviews of all.

Appendix 1: Incident Report Form

Description of the Data Breach	
Time and Date breach was identified and by whom	
Who is reporting the breach: Name	
Contact details: Telephone/Email	
Classification of data breached i. Public Data ii. Internal Data iii. Confidential Data iv. Highly confidential Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing what actions are being taken to recover the data	
Who has been informed of the breach	
Any other relevant information	

Email form to spectrum@spectrumanalysis.com.au
Call +61 398300077 and / or 0411 604921 and advise that a Data Security Breach report form is being sent.

Received by:	
Date/Time:	

Appendix 2: Evaluation of Incident Severity

The severity of the incident will be assessed per the standard IS Incident Management by the Chief Data Scientist at Spectrum Analysis. Assessment would be made based upon the following criteria:

High Criticality: Major Incident	**Contact:**
• Highly Confidential/Confidential Data • Personal data breach involves > 1000 individuals • External third party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response beyond normal operating procedures	Peter Buckingham Managing Director – Spectrum Analysis Ph 0411 604921 Other relevant contacts • Chief Data Scientist – Spectrum Analysis • Ph 0433 217720 • Contact external parties as required ie police/OAIC/individuals impacted
Moderate Criticality: Serious Incident	**Contact:**
• Confidential Data • Breach involves personal data of more than 100 individuals • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Incident does not require immediate response	Peter Buckingham Managing Director – Spectrum Analysis Ph 0411 604921 Other relevant contacts • Chief Data Scientist – Spectrum Analysis • Ph 0433 217720 • Contact external parties as required ie police/OAIC/individuals impacted
Low Criticality: Minor Incident	**Contact:**
• Internal or Confidential Data • Small number of individuals involved • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted • Incident can be responded to during working hours *Example:* • *Email sent to wrong recipient* • *Loss of encrypted mobile device*	• Chief Data Scientist – Spectrum Analysis • Ph 0433 217720

Appendix 3: Data Breach Checklists

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Step	Action	Notes
A	**Containment and Recovery:**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Managing Director – Spectrum Analysis to ascertain the severity of the breach and determine if any personal data is involved.	**See Appendix 2**
2	Chief Data Scientist – Spectrum Analysis to identify Lead Responsible Officer for investigating breach and forward a copy of the data breach report	To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority.
3	Identify the cause of the breach and whether the breach has been contained? Ensure that any possibility of further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant persons who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
5	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
6	Where appropriate, the Managing Director Spectrum Analysis or nominee to inform the police.	E.g. stolen property, fraudulent activity, offence under Crimes Act.
7	Ensure all key actions and decisions are logged and recorded on the timeline.	

Step	Action	Notes
B	**Assessment of Risks**	**To identify and assess the ongoing risks that may be associated with the breach.**
8	What type and volume of data is involved?	Data Classification/volume of individual data etc
9	How sensitive is the data?	Identify what level of data has been breached
10	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
11	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
12	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies.
13	How many individuals' personal data are affected by breach?	
14	Who are the individuals whose data has been compromised?	Customers, clients or suppliers?
15	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
16	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft/fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?
17	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
18	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Step	Action	Notes

C	Consideration of Further Notification	Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.
19	Are there any legal, contractual or regulatory requirements to notify?	E.g.: terms of funding; contractual obligations
20	Can notification help Spectrum Analysis meet its security obligations?	E.g. prevent any unauthorised access, use or damage to the information or loss of it.
21	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
22	Is there a need to inform the Office of the Australian Information Commissioner?	Contact and liaise with the Director of Office of the Australian Information Commissioner.
23	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work".
24	Consider whom to notify, what you will tell them and how you will communicate the message.	• There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. • Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. • When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. • Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).
25	Consult the AIOC guidance on when and how to notify it about breaches.	There should be a presumption to report to the AIOC where personal data is concerned and there is a real risk of individuals suffering some harm.
26	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

Step	Action	Notes

D	Evaluation and Response	To evaluate the effectiveness of Spectrum Analysis' response to the breach.
27	Establish where any present or future risks lie.	
28	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
29	Consider and identify any weak points in existing security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
30	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
31	Report on findings and implement recommendations.	Report to Managing Director – Spectrum Analysis.

Appendix 4: Timeline of Incident Management

Date	Time	Activity	Decision	Authority