Data Breach Response Plan

Data Analytics Centre

Purpose

The Data Breach Response Plan sets out the process to be followed by Data Analytics Centre (DAC) staff in the event of a data breach.

1. Legislative and policy context

While NSW does not currently have a mandatory notifiable data breach reporting requirement, the Privacy Commissioner has a voluntary scheme in place. The voluntary scheme encourages agencies that have experienced a serious data breach to report the details of the breach to the Privacy Commissioner, so that the Privacy Commissioner can assess the breach, provide advice or investigate.

If DAC receives personal or health information under the *Data Sharing (Government Sector) Act 2015* and it becomes aware that the privacy legislation has been (or it is likely to have been) breached, it must inform the agency that provided the data and the Information Privacy Commissioner (IPC) as soon as practicable.[1]

2. Definition of a data breach

A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, the data.

A data breach may occur through:

- The accidental loss or theft of data or information (including a hard copy)

[1] *NSW Public Sector Agencies and Notifiable Data Breaches*, Fact Sheet, Information and Privacy Commission New South Wales, February 2018

- The transfer of sensitive or confidential information to those who are not authorised to receive that information
- Attempts (either failed or successful) to gain unauthorised access to data, information systems or a computing device
- Changes to information or data, system hardware, firmware, or software configuration without DAC's knowledge, instruction or consent
- Unwanted disruption or denial of a service to a system
- The unauthorised use of a system by any person
- The loss of service

3. Potential impacts of a data breach

The impact of a data breach depends on the nature and extend of the breach and the type of information that has been compromised. Serious impacts of a breach could include:

- Risks to individuals' safety
- Financial loss to an individual or organisation
- Damage to personal reputation or position
- Loss of public trust in the DAC and/or the Agency providing the data
- Commercial risk through disclosure of commercially sensitive information to third parties
- Threat to DAC systems, leading to disruption of activities
- Impact on Government reputation, finances, interests or operation

It is important to note that breaches of personal data can result in significant harm, including people having their identity stolen or the private home addresses of vulnerable people being disclosed. As such, even a breach affecting an individual or a small number of people may have a large impact.

4. Process for responding to a data breach

The following steps outline the process which must be followed by DAC staff in relation to any breach incident, including a suspected but unconfirmed incident.

Step 1: Alert

Where a data breach is known to have occurred (or is suspected) any member of DAC staff who becomes aware of the breach must immediately alert (by phone) the Data Governance Team and the DAC Leadership Team.

Where possible, the staff member who discovered the breach should try and provide the following information:

- Contact name and number of persons reporting the incident
- The type of data or information involved
- Whether the loss of the data puts any person or other data at risk
- Location of the incident
- Date and time the breach occurred
- Location of data or equipment affected
- Type and circumstances of the incident

It is important to note that the staff member who discovered the breach should alert these teams immediately, and not wait until all the key details on the breach have been established.

If the staff member who discovers the breach is authorised by the DAC to take action to contain the breach, they must act as soon as possible to contain the breach and minimise the damage. This may involve:

- shutting down of applications
- closing of accounts
- changing passwords
- attempting to locate missing items, or
- restricting access rights.

Please note that not all staff will be authorised to take these actions, and containment should only be enacted by authorised staff.

Step 2: Verification

Once notified of any data breach, the Data Governance Team must quickly establish the key details of the breach, including when it occurred or was identified, how it occurred, what data was affected and the extent of the breach.

The Data Governance Team must also consider whether the data breach involves personal or health information and provide findings to the DAC Leadership Team and the Service Management Team.

Step 3: Impact Assessment

The Service Management Team is then responsible for determining the seriousness of the data breach. While there is no objective measure of seriousness, the Service Management Team will need to work out what constitutes a serious breach by considering:

- The type of data held
- Whether personal or health information was disclosed
- The number of individuals affected
- The risk of harm that could be caused to both individuals and the DAC by the breach.

In assessing the seriousness of the breach, the Service Management Team will need to consider:

- **The type of data that has been breached** – does it include financial, health or other sensitive categories of data? Are there other characteristics of the data that could pose a high risk (e.g. commercial information that could pose a reputational risk to an Agency or another organisation?)
- **The data context** – does the breach affect data that would normally be publicly available, or is the data known to be very poor quality that if used could create risk to individuals?
- **How easy would it be for individuals to be identified from this data**?
- **The circumstances of the breach** – for example, was it a single incident (such as the loss of a laptop) or a malicious attack that poses an ongoing risk, or was the data altered in a way that it would pose a risk to the individuals to whom the data relates?

The responses to these questions, and assessment of the overall impact of the breach, are to be reported to the DAC Leadership team, Cluster Chief Information Security Officer (CISO) and the Cluster Chief Information Officer (CCIO).

The Service Management Team is also responsible for logging the incident in the cluster's Information Security Management System (ISMS) for record management purposes.

Step 4: Rectification

The Service Management Team must take steps to eliminate the circumstances enabling the breach. This could include actions such as initiating take down orders on external websites or putting processes in place to assist individuals who have been affected by the breach.

The steps of the rectification process must be reported to the CISO and CCIO for documenting with ISMS.

Step 5: Notification

DAC Leadership Team must notify, as appropriate, the cluster Deputy Secretary and external customers (i.e. the data owner) and NSW Privacy Commissioner of the data breach as soon as practicable.

For instances where information is shared from one or more NSW Government agencies to the DAC, and the data breach includes health information or personal information, *the Data Sharing (Government Sector) Act 2015* requires that both the data provider and the Privacy Commissioner be notified as soon as practicable. An example of what should be included in the report to the Privacy Commissioner can be found in the IPC's Data Breach Policy.

While individuals and organisations affected by a serious data breach should be notified as soon as practicable, in instances where the DAC is not the owner of the data (i.e. the data has been provided by another agency), it is more appropriate for the agency that provided the data to notify affected individuals.

Step 6: Review

Once the matters referred have been dealt with, the Data Governance Team and the Service Management Team should identify lesson learned and remedial action that can be taken to reduce the likelihood of recurrence.

This might include a review and remediation of:

- The internal controls in place
- Policies and procedures
- Staff skills and refresher training
- Contractual obligations with contracted service providers.

The DAC Leadership Team, CISO and the CCIO should be contacted for advice. The DCS Information Privacy Team should also be consulted if the breach includes personal or health information.

5. RACI

The section below lists the responsibilities and roles of DAC teams when a breach occurs or is suspected.

Process	Incident Identifier	Data Governance	Service Management	DAC Leadership	Cluster Chief Information Security Officer (CISO)	Cluster Chief Information Officer (CIO)	Deputy Secretary	Data Owner	Privacy Commissioner
Alert	R	I	I	I	N/A	N/A	N/A	N/A	N/A
Verification	I	RA	C	I	N/A	N/A	N/A	N/A	N/A
Impact Assessment	I	C	RA	I	I	I	N/A	N/A	N/A
Rectification	C	C	RA	I	C	C	N/A	N/A	N/A
Notification	I	C	C	RA	I	I	I	I	I
Review	C	RA	RA	C	C	C	I	I	N/A

R: Responsible **A**: Accountable **C**: Consult **I**: Inform **N/A**: Not applicable

6. References

- NSW Cyber Security Policy
- NSW IPC Data Breach Guidance
- NSW IPC Data Breach Policy

7. Monitoring, Evaluation and Review

Monitoring:	DAC Data Governance team will undertake ad hoc observations and audits of the Data Breach Response Plan.
Evaluation and review:	The Response Plan will be reviewed bi-annually or in the event of legislative or policy changes relating to data breach notifications.

8. Version Control and Change History

Date	Version	Approved by	Amendment
April 2019	1		Initial issue
April 2020	2		Second issue