Data Security Incident and Breach Policy

McMillan Shakespeare Group of Companies

Legal and Compliance

Reviewed and Adopted by the Board on 29 July 2024

Document Owner	**Group General Counsel**
Version Control	**Version 5.3 July 2024**
Last Reviewed	**Legal and Compliance– July 2024**
Approved by the Board	**29 July 2024**
Policy Review Frequency	**Triennially (or as per section 7)**
Audience	**MMS Internal**
Publication	**Internal (Intranet)**

Table of Contents

1. Scope

This policy applies to McMillian Shakespeare Limited and its subsidiary companies and businesses (**MMS**)and to all data security incidents regardless of severity and how the incident occurred (i.e. whether the incident involves MMS Group IT systems or not). All persons employed by or representing MMS including directors, officers, employees, and contractors, whether full time, part time or casual (collectively "**MMS Staff**") are required to comply with this policy.

2. Background

This policy aims to ensure that data security incidents and breaches are handled in accordance with applicable legal requirements under the:

- *Privacy Act 1988 (Cth)* (**Privacy Act**) and related legislation, including the requirements of the Notifiable Data Breaches (**NDB**) scheme in Part IIIC of the Privacy Act.
- *Privacy Act 2020 (NZ)* (**NZ Privacy Act**) and Part 6 of the NZ Privacy Act – Notifiable Privacy Breaches.

3. Identifying Data Security Incidents

3.1. What is Data?

Data covers any information irrespective of whether it relates to a company or an individual, for example, information about MMS, customer data, employee data, supplier data or personal information.

3.2. What is a Data Security Incident?

A **Data Security Incident** is an error or occurrence where the security of any data held by McMillan Shakespeare (**MMS**) is compromised and results in:

- **potential** unauthorised access, disclosure or use of the data, or the data is potentially lost in circumstances where it is likely for unauthorised access, disclosure or use to occur; and
- the impact is or is likely to be *insignificant or minor.*

For the purpose of this Policy:

- a Data Security Incident can be caused by an unknown third party (e.g. hackers) and is not limited to an error made by MMS or its contractors;
- a Data Security Incident may involve a failure of a material condition under a contract or a deviation from a MMS's policy or procedure; and
- a Data Security Incident **does not** involve non-compliance with legislation, a condition of any licence or registration held by MMS or any other regulatory requirement.

For clarity a Data Security error or occurrence is classified as an Incident **where there is no unauthorised access, disclosure or use of personal information.**

Personal Information is any information or an opinion:

- about any individual person who is identified; or
- that is reasonably identifiable ((e.g. a person's name in combination with additional information such as the person's contact details, bank account details, credit card details, tax file numbers, employment and payroll details and 'sensitive information' about their race, religious belief, sexual orientation, criminal record); whether the information is true or not; and
- whether the information or opinion is recorded in a material form or not (e.g. voice recordings and biometrics data (if they identify an individual or can reasonably identify an individual).

3.3. What is a Data Security Breach?

A **Data Security Breach** is an occurrence where the security of any data held by MMS is compromised and involves:

- non-compliance with legislation, a licence or registration condition or any regulatory requirement;
- **actual** unauthorised access, disclosure or use of the data, or the data is lost in circumstances where it is likely for unauthorised access, disclosure or use to occur; and
- any data irrespective of whether it relates to MMS, a company or to an individual.

A **Low Impact Data Security Breach** is a Data Security Breach where the impact is not or is not likely to result in serious harm to the affected party.

In contrast, a **High Impact Data Security Breach** is where the impact is or is likely to result in serious harm to the affected party.

3.4. What is a Notifiable Data Security Breach (NDB)?

A NDB is a High Impact Data Security Breach which involves Personal Information (as set out in section 1.1 of this Policy) and is notifiable under Part IIIC of the Privacy Act and Part 6 of the New Zealand Privacy Act (2020)

Accordingly, a NDB occurs (and is notifiable to the Office of the Australian Information Commissioner (**OAIC**) and the New Zealand Office of the Privacy Commissioner) when:

- the data *involves Personal Information of an individual*;
- there is actual unauthorised access, disclosure or use of the Personal Information, or the Personal Information is lost in circumstances where it is likely for unauthorised access, disclosure or use to occur;
- a reasonable person would conclude that the access, disclosure or use (or the likely access, disclosure or use) would be likely to *result in serious harm* to any of the *individuals* to whom the information relates; and
- the organisation has not been able to prevent the likely risk of serious harm with remedial action.

Unlike a Data Security Breach, a NDB must involve Personal Information of an individual and the serious harm affects or is likely to affect an individual.

A NDB is deemed by the Privacy Act and Privacy Act NZ to not be a breach if before the access or disclosure (or before the likely access or disclosure) results in serious harm, MMS takes action in relation to the access or disclosure and as a result of such action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of the impacted individuals.

4. Responding to Data Security Incidents / Breaches

4.1. General Principles

The OAIC and the NZ Privacy Commissioner have recommended 4 key steps to undertake when a Data Security Breach has occurred. For the purpose of this Policy, the 4 key steps shall apply to Data Security Incidents as well.

The 4 key steps are:

- containment – taking steps to prevent any further compromise of the data (which may involve ongoing revision or update containment steps, as new information comes to light);
- assessment – gathering the facts and assessing the risks of the occurrence of the Data Security Incident/Breach, including any actual or potential harm to affected parties before and after containment steps are taken);
- notification – notifying individuals and the OAIC (if required); and
- review/prevention – considering and preventing further future incidents/breaches.

The OAIC and New Zealand Privacy Commissioner expect entities to undertake remedial action where possible to limit the impact of the Data Security Breach on affected individuals.

In addition to the 4 key steps, consideration will also be given to the Cyber Security Incident Response Plan (**CSIRP**) and Crisis Management Framework (**CMF**) procedures to provide a controlled and coordinated approach to handling a Data Security Incident or Breach (refer to section 4.2 below).

4.2. Containment and Assessment

If a **Low Impact** Data Security Incident or Data Security Breach is suspected to have occurred, or may have occurred, the MMS Staff member who identified it or was notified about it must notify their Team Leader/Manager on the same business day that the matter comes to their attention. In turn the Team Leader/Manger will as soon as practicable notify their Designated Officer, who (in addition to their responsibilities referred to below) may liaise with the Group Privacy Officer or a member of Legal and Compliance for guidance and assistance.

The **Designated Officer** (defined in the MMS Business Incident and Breach Reporting Policy) is the nominated employee from each MMS business, responsible for:

- reviewing each business incident and breach, including compensation and good will payments, for accuracy and completeness; and
- reporting breaches to the Compliance for possible inclusion in the MMS Breach Register.

If a **High Impact** Data Security Breach or a NDB is *suspected* to have occurred, or may have occurred, the

MMS Staff member who identified it or who was notified about it must **immediately** notify their Team Leader/Manager, who will in turn immediately notify the Designated Officer as well as the relevant Executive Leadership Team (**ELT**) Member (being a direct report of the MMS CEO), the Group Privacy Officer, Group General Counsel and Head of Risk.

The relevant ELT Member will determine whether to invoke the CMF procedures and their respective Crisis Response Team (**CRT**) and liaise with the Cyber Security Incident Response Team (**CSIRT**) to investigate and propose containment options.

The relevant ELT Member, together with the ELT Member for IT (if required) must take immediate steps in all cases to:

- contain the suspected Data Security Incident/Breach; and
- gather all relevant information about the matter (e.g. the cause, the nature of the data, who has been impacted and potential harm (including economic, psychological, physical harm).

Group Legal along with the Group Privacy Officer will assess the matter to determine whether a NDB has occurred.

4.3. Executive Response Team

If a Data Security Breach or a NDB may have occurred, the relevant ELT Member must immediately notify the MMS CEO who will determine: (a) whether it is necessary to convene the Executive Response Team (**XRT**) and (b) whether urgent regular reporting to the Board (or Chair of the Board) is necessary.

The purpose of the XRT is to provide additional management oversight of, and input into, an appropriate response to the suspected Breach including a consideration of:

- remedial actions proposed by the CSIRT;
- communication strategy;
- management of any reputational consequences to MMS;
- implementation of any particular operational protocols (e.g. preservation of evidence, protection of legal professional privilege) or customer protocols;
- notification to insurers (if applicable); and
- communication with the OAIC / NZ Privacy Commissioner and any other applicable regulator such as the ASIC, ASX or NDIS Commission.

Where the CMF procedures are invoked, the CRT and CSIRT must provide regular situational reports to the XRT chaired by the MMS CEO.

4.4. Notification and Review

The MMS CEO or the XRT (if applicable) must assess having regard to legal advice, *whether there are reasonable grounds to believe that the relevant circumstances amount to a Notifiable Data Security Breach*. The assessment must be completed within 30 days of MMS having reasonable grounds to form its suspicion.

It is possible for circumstances to arise such that a belief (as distinct from a suspicion) is formed from the

outset, in which case the same processes described in sections 4.2, 4.3 and 4.4 will apply except that the 30 day assessment period would not be required.

As a separate matter, Group Legal should also consider whether a criminal offence has occurred and, in conjunction with the relevant business unit and its ELT Member, determine whether there are any relevant contractual obligations that may be triggered as a result of the incident or breach.

If it has been assessed *that there are reasonable grounds to believe that the relevant circumstances amount to a Notifiable Data Security Breach*, the following steps must be taken:

- Group Legal, with relevant stakeholder input, must prepare a statement in accordance with s.26WK of the Privacy Act and provide that statement to the OAIC (or NZ Privacy Commissioner for NZ NDBs) as soon as practicable; and

- the relevant ELT Member must make sure that impacted individuals are notified of the content of the statement or if that is not practicable, then, check that a copy of the statement is published on the relevant MMS website and reasonable steps are taken to publicise the contents of the statement.

  (Note: if within the 30 day assessment period, it is assessed that there are reasonable grounds to believe that a NDB has occurred, MMS must consider its notification obligations immediately and not wait until the end of the 30 day period.)

MMS should also conduct a review of the Data Security Breach or NDB (as the case may be) with a view to improving its handling of Personal Information and strengthening its security measures. A review may include but is not limited to the following considerations:

- root cause analysis of the breach;

- a plan to prevent similar breaches from occurring in the future;

- monitoring or audits to confirm that the prevention plan is implemented;

- a review of policies and procedures;

- changes to employee selection and training practices; and

- a review of service delivery partners who were involved in the breach (if any).

5. Record Keeping

Each Business is responsible for retaining sufficient records of data security events.

Team Leaders / Managers within each MMS business are required to implement processes suitable to their teams for managing data security incidents and breaches. The implemented process must include the:

- identification;
- assessment (incident / breach, nature, scale, root cause and impact);
- remediation (corrective or preventative actions to mitigate or eliminate the impact of the incident / breach, and likelihood of recurrence. When appropriate, rectifying loss or damage as required);
- recording; and
- reporting.

All Data Security Breaches must also be recorded in the MMS Breach Register maintained by Group Compliance. This register includes NDB assessments completed by Group Legal, which record the assessment and the factual basis underpinning the assessment. To the extent that this Register contains any legal advice, legal professional privilege shall apply over such advice.

6. Policy contraventions

Any serious or repeated contraventions of this policy may result in disciplinary action in line with the MMS Disciplinary Policy and Process. Disciplinary action may include a written warning up to the termination of employment (for employees) or termination of engagement (in the case of independent contractors or consultants).

If you become aware of another MMS Staff member failing to comply with this policy please report the matter to your Team Leader/Manager as soon as practicable.

7. Related MMS Codes, Frameworks, Policies and Processes

This is not a stand-alone policy/framework but operates in conjunction with other MMS codes, frameworks and policies which include:

- MMS Cyber Security Incident Response Plan;
- MMS Relevant business units Business Continuity Plans;
- MMS Privacy Policy;
- MMS Continuous Disclosure and Shareholder Engagement Policy;
- MMS Whistleblower Policy;
- MMS Compliance Framework; and
- MMS Breach and Incident Reporting Policy.

8. Review of Policy

Group Legal is responsible for periodically reviewing this Data Security Incident and Breach Policy, no less than once every 3 years