STADIUMS QUEENSLAND

Data Breach Policy

GABBA · SUNCORP STADIUM · cbus super stadium · People First Stadium · Queensland Country Bank Stadium · Brisbane Entertainment Centre · QSAC · QTC Queensland Tennis Centre · Sleeman Sports Complex

Contents

1 Purpose 3
2 Application 3
3 Definitions 3
4 Roles and Responsibilities 4
5 Responding to a Data Breach 6
5.1 Stage 1: Preparation 6
5.2 Stage 2: Identification 6
5.3 Stage 3: Containment and Mitigation 7
5.4 Stage 4: Assessment of Data Breaches 8
5.4.1 Assessment to determine whether a Data Breach is an Eligible Data Breach 8
5.4.2 Mitigation of Serious Harm 9
5.4.3 Recording Eligible Data Breaches 10
5.5 Stage 5: Notification Requirements 10
5.5.1 Data Breach 10
5.5.2 Eligible Data Breach 10
5.5.3 Exemptions to notification requirements 11
5.6 Stage 6: Post data breach review and remediation 11
6 Record Keeping 12
7 Human rights compatibility 12
8 Related legislation and policies 12
9 Document management 13
10 Revision history 13
11 For more information 13

1 Purpose

This Data Breach Policy (Policy) sets out an overview of how Stadiums Queensland (**SQ**) will respond to a Data Breach, including a suspected Eligible Data Breach, in accordance with the Mandatory Notification of Data Breach (**MNDB**) scheme under the *Information Privacy Act 2009* (Qld) (**IP Act**).

This Policy has been prepared in accordance with section 73 of the IP Act. It sets out the framework for SQ's compliance with the MNDB scheme and details the procedure by which SQ identifies, responds to, notifies and reports, and manages actual or suspected Data Breaches. This Policy is designed to aid SQ in facilitating a timely and effective response to a Data Breach, in turn avoiding or mitigating potential harms to affected individuals and reducing the risks to SQ.

2 Application

This Policy applies to all staff (including contractors) and third-party service providers of SQ that access, store, process, or transmit personal information, other confidential business information, or other data critical to SQ.

3 Definitions

The following definitions apply to this Policy:

Affected individual is an “affected individual” under section 47(1)(ii) of the IP Act.

Data Breach refers to unauthorised access to, or unauthorised disclosure of information, or the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

Data User means all staff (including contractors) and third-party service providers of SQ that access, store, process, or transmit personal information, other confidential business information, or other data critical to SQ.

Eligible Data Breach occurs where:

(a) there has been unauthorised access to, or unauthorised disclosure of Personal Information Held by SQ, and the access or disclosure is likely to result in Serious Harm to any of the individuals to whom the information relates; or

(b) there has been loss of Personal Information Held by SQ that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, and the loss is likely to result in Serious Harm to any of the individuals to whom the information relates.

Held or **hold** in relation to personal information means personal information is held by a relevant agency, or the agency holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant agency.

MNDB means mandatory notifiable data breach (under which entities are required to notify of Eligible Data Breaches).

Personal Information or **PI** means information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Privacy Officer refers to the individual responsible for organisational compliance with privacy laws and regulations. The Information Management Coordinator is the Privacy Officer for SQ.

Serious Harm to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example:

(a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or
(b) serious harm to the individual's reputation because of the access or disclosure.

4 Roles and Responsibilities

To ensure that SQ staff are and remain aware of their obligations under the MNDB Scheme, SQ endeavours to (as appropriate):

- Prepare and notify staff of this Policy and the Data Breach Response Plan; and
- Provide training on this Policy and the Data Breach Response Plan

Role	Responsibilities
Data User	• Read this Policy and Data Breach Response Plan and understand what is expected of them. • Comply with the IP Act, including protecting personal information held by SQ from unauthorised access, disclosure or loss. • Where required in accordance with this Policy, immediately report a Data Breach or suspected Data Breach to the Privacy Officer. Reporting may also be required to Technology Services where required under the Cyber Security Incident Response Plan. • Respond to requests for information from, and cooperate with, the Privacy Officer and the Data Breach Response Team (**DBRT**). • Comply with record keeping obligations.
Privacy Officer	• Assess the severity of a Data Breach and the likelihood that a Data Breach will result in Serious Harm to an individual to whom the information involved relates. • Escalate serious Data Breaches to the DBRT in accordance with the Data Breach Response Plan. • Where relevant, manage notification of the Eligible Data Breach to the Queensland Information Commissioner and other Affected Individuals. This includes ensuring publishing, monitoring and reviewing the currency of public notifications of an Eligible

	Data Breach published to SQ's website, in accordance with the process set out in the Data Breach Response Plan. • Maintain the Register of Eligible Data Breaches. Maintain, test, and review this Policy and the Data Breach Response Plan. • Undertake post data breach review.
SQ Manager	• Identify and escalate concerns within the Manager's area of responsibility which may enliven the requirements of this Policy. Where required in accordance with this Policy, immediately report a Data Breach or suspected Data Breach to the Privacy Officer. Reporting may also be required to Technology Services where required under the Cyber Security Incident Response Plan.
Group Executive, Finance and Corporate Services	• Promotes compliance with the MNDB Scheme. • Stand up the DBRT (where required) and nominate a response coordinator to be the DBRT Lead. • Where two or more policies apply, make decisions on a response strategy which ensures efficiency and avoids duplication. • Make notifications in relation to data breaches with support from the Privacy Officer and General Counsel.
Data Breach Response Team (**DBRT**)	• Manage a Data Breach in accordance with the Data Breach Response Plan. • Where relevant, manage the publishing, monitoring and reviewing the currency of public notifications of an Eligible Data Breach published to SQ's website, in accordance with the process set out in the Data Breach Response Plan, in conjunction with the Privacy Officer and General Counsel. • Where required, due to the nature of the specific breach, liaise with the SQ's Cyber Security Incident Response Team (**CSIRT**) and / or SQ's Crisis Management Team (**CMT**).
DBRT Lead	• Will be the Group Executive, Finance and Corporate Services, or other person as nominated by the Group Executive, Finance and Corporate Services. • Assist the Group Executive, Finance and Corporate Services in the standing up and supporting a DBRT. • Assist the DBRT in coordinating the agency response.
Communications Manager	• Publish, monitor and review the currency of public notifications of Data Breaches published to the SQ website

5 Responding to a Data Breach

5.1 Stage 1: Preparation

SQ has established a range of processes and procedures to prevent, respond to, and manage Data Breaches (including Eligible Data Breaches).

SQ has developed and maintains the following documents for internal use:

- A Data Breach Response Plan which provides step-by-step, practical guidance regarding how SQ will respond to a Data Breach in accordance with this Policy;
- Several Data Breach Response Playbooks, which are operationally focused procedures and checklists that provide a clear set of actions for specific incident types;
- An Information Privacy Policy which provides guidance to SQ staff around the handling and storage of personal information; and
- A Cyber Security Incident Response Plan and Playbooks which provide step-by-step, practical guidance on how SQ will respond to a cyber incident (which may include a Data Breach).

To ensure a unified approach, SQ's Data Breach response and recovery process is integrated into SQ's cyber response, incident, emergency and business continuity arrangements and communications strategies.

SQ has a DBRT, and various staff assigned with Data Breach incident response responsibilities. SQ may also engage other parts of the organisation (including its CSIRT and CMT) and/or outsourced service providers to manage complex incidents. These roles and responsibilities are outlined in section 4.

The DBRT is a cross-functional team responsible for coordinating the response to actual or suspected Data Breaches, comprising of the Group Executive Finance and Corporate Services, DBRT Lead, the Privacy Officer, General Counsel, Communications Manager and subject matter experts within SQ. The responsibilities and reporting lines of the DBRT are outlined in section 4. Further detailed guidance about the DBRT, its composition and specific responsibilities is contained in the Data Breach Response Plan.

SQ endeavours to:

- Where practical or appropriate based on risk based assessments, include Data Breach management and notification obligations in its service provider contracts and agreements;
- Provide training and awareness for its staff in identifying and managing Data Breaches; and
- Test and review this Policy and the Data Breach Response Plan at least annually and in response to an Eligible Data Breach.

5.2 Stage 2: Identification

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.

Common indicators of a Data Breach may include:

- Alerts from security systems or monitoring tools (e.g., security monitoring, network monitoring, intrusion detection / prevention systems, etc.);

- Reports from staff or customers (e.g., misdirected emails, suspicious activity);
- Notifications from third-party service providers, partners, or government agencies;
- Media reports or public disclosures.
- Examples of incidents that may result in a Data Breach include, but are not limited to, the following:
    - Lost or stolen laptops, USB drives, or mobile devices containing Personal Information;
    - Misdirected emails containing customer data;
    - Unauthorised access to internal databases or systems;
    - Cyber-attacks such as phishing, ransomware, or account compromise.

All Data Users are responsible for reporting suspected or actual Data Breaches as soon as they become aware of them.

All Data Breaches, either suspected or actual, must be reported to as soon as possible, and must be documented and prioritised immediately upon receipt, to SQ's Privacy Officer: RTI-privacy@stadiums.qld.gov.au

The Privacy Officer, together with General Counsel, will use their discretion in recommending to the Group Executive, Finance and Corporate Services whether a Data Breach or suspected Data Breach requires escalation to the DBRT.

5.3 Stage 3: Containment and Mitigation

Once a suspected (or actual) Data Breach is identified, SQ will take reasonable steps to contain and mitigate the Data Breach. These steps may include:

- Conducting a risk assessment of the Data Breach;
- Adopting an appropriate approach based on the level of risk assessed;
- Convening the DBRT to assist in containing, mitigating and assessing the Data Breach;
- Liaising with the CSIRT, subject matter experts and/or other appropriate departments to contain the Data Breach;
- Considering whether to involve external parties, such as statutory authorities;
- Considering requirements to inform or involve third parties, such as service providers, organisations and agencies; and
- Undertaking remedial actions to address the Data Breach, such as:
    - Recovering data;
    - Remote wiping lost devices; and
    - Denying access to lost data.

The risk assessment process will involve evaluating a suspected Data Breach to identify low (smaller scale / minor), medium and high risk (more significant / Suspected Eligible Data breach) Data Breach scenarios. The following factors may inform the risk assessment:

- Nature and sensitivity of information;
- Amount of information and number of affected individuals;
- Ease of identifying the individuals;
- Seriousness of the harm; and

- Existing mitigating measures.

Each risk level requires a different approach, and this risk assessment will inform containment and mitigation strategies. The following considerations may inform which containment measures need to be taken:

- What happened to cause the incident;
- Can interim controls be implemented;
- How serious is the incident (i.e. what information and individuals are impacted);
- Does SQ need to work with any third parties to investigate and resolve the incident;
- Is internal assistance from other business areas required (e.g. information security);
- Can the personal information be recovered;
- Can the person who has received information incorrectly be contacted;
- Can the system which has been breached be shut down;
- Can the activity that led to the breach be stopped;
- Can access codes or passwords be revoked or changed; and
- Did the data breach occur due to the actions of an external party (i.e. a cyber-attack).

The DBRT is responsible for leading the Data Breach response effort, including the containment and mitigation phase.

SQ's containment and mitigation of a Data Breach may also be supported by procedures under the Cyber Security Incident Response Plan.

5.4 Stage 4: Assessment of Data Breaches

5.4.1 Assessment to determine whether a Data Breach is an Eligible Data Breach

SQ must assess whether a Data Breach is an Eligible Data Breach within 30 days of forming a reasonable suspicion of a Data Breach having occurred. However, this time may be extended in accordance with section 49 of the IP Act. Where the Data Breach is a Data Breach of more than one agency (and that other agency has complied with the MNDB scheme), SQ is not required to assess the Data Breach under section 56 of the IP Act.

SQ’s assessment of whether a Data Breach is an Eligible Data Breach, will be conducted by gathering and assessing all available information about the Data Breach, including:

- The type of information involved;
- The sensitivity of that information;
- Whether the breach involves unauthorised access to, or unauthorised disclosure of personal information;
- How or if the information is protected and the likelihood of those controls being overcome;
- How the breach occurred;
- The persons who have or could obtain that data;
- The likelihood of misuse;
- Potential harm to individuals including how easily individuals can be identified from the information;

- The nature of such harm to individuals (identity theft, financial loss, physical safety, loss of business or employment, humiliation, reputation, relationships, marginalisation, or social bullying, etc.);
- The seriousness of harm that is likely as a result of the Data Breach;
- Whether there are any mitigations.

Harm is to be assessed from the lens of anticipated consequence on individuals and the likelihood of the harm eventuating.

Harm can encompass any (or multiple) of the following harms:

- Physical;
- Psychological;
- Emotional;
- Financial; or
- Reputational.

SQ will consider the following in assessing the seriousness of the Data Breach:

- What is the nature of the breach;
- Is it likely that a counterparty or third party caused the breach;
- Has the breach affected another agency;
- Are there any vulnerabilities of the affected individuals e.g. involving children or a domestic violence victim-survivor;
- The effectiveness of the steps taken to control the breach e.g. has containment and mitigation lessened the risk;
- Has there been unauthorised access, disclosure or loss of personal information that was collected by the agency; and
- If so, would a reasonable person conclude the breach is likely to result in serious harm to an individual to whom the information relates.

SQ will use the available information to assess the cause and extent of the Data Breach and determine priorities and risk. SQ will undertake a holistic assessment considering each of the Serious Harm indicators to determine:

- The type or types of personal information involved in the Data Breach;
- The circumstances of the Data Breach; and
- The nature of the harm that may result from the Data Breach.

5.4.2 Mitigation of Serious Harm

If SQ takes positive steps to address a Data Breach, in a timely manner, such that Serious Harm is unlikely to occur, then they are not obliged to notify affected individuals or the Queensland Information Commissioner. Factors which may indicate that Serious Harm has been remediated include:

- SQ has taken action to mitigate the harm caused by the Data Breach / loss of data;
- Such action is taken before there is access or disclosure to the personal information; and

- As a result of the action taken, the Data Breach is no longer likely to result in Serious Harm to any individual.

5.4.3 Recording Eligible Data Breaches

Records of the assessment, including any actions taken and decisions made, should be recorded in an Incident Log. Data Breaches which are assessed to be an Eligible Data Breach must be recorded in SQ's Register of Eligible Data Breaches.

5.5 Stage 5: Notification Requirements

5.5.1 Data Breach

If SQ assesses that a Data Breach has occurred in respect of one or more individuals, SQ will consider whether to notify any individuals affected by the breach. The Privacy Officer, in conjunction with the General Counsel, will determine notification requirements.

The Communications Manager will arrange communication with external parties affected, and the affected individuals as applicable.

SQ endeavours to be clear, accurate and transparent in its communications in respect of a Data Breach.

Other entities may be notified if required, such as:

- Law enforcement;
- Regulators;
- The Australian Signals Directorate (ASD) & the Australian Cyber Security Centre (ACSC);
- Insurance providers;
- Other relevant entities.

5.5.2 Eligible Data Breach

If SQ assesses that an Eligible Data Breach has occurred in respect of one or more individuals, (unless an exemption applies:

- The Privacy Officer, in conjunction with the General Counsel, will determine notification requirements;
- As soon as practicable, the Privacy Officer will prepare and provide the Queensland Information Commissioner with a statement which complies with the IP Act;
- As soon as practicable, the Communications Manager will arrange notification to individuals affected by the breach, which may involve publishing the information provided to the Queensland Information Commissioner on the SQ website if the individuals cannot be contacted directly; and
- The Communications Manager will arrange communication with external parties affected, such as stakeholders, contractors or other third parties.

SQ endeavours to be clear, accurate and transparent in its communications in respect of an Eligible Data Breach, communications in the event of an Eligible Data Breach will also occur in accordance with communications guidance in the Data Breach Response Plan.

Other entities may be notified if required, such as:

- Law enforcement;
- Regulators;
- The Australian Signals Directorate (ASD) & the Australian Cyber Security Centre (ACSC);
- Insurance providers;
- Other relevant entities.

5.5.3 Exemptions to notification requirements

SQ will be exempt from complying with the notification requirements under the IP Act in respect of an Eligible Data Breach if complying with the notification requirements:

- Is likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal;
- Would be inconsistent with a provision of an Act of the Commonwealth or a State that prohibits or regulates the use or disclosure of the information;
- Would create a serious risk of harm to an individual's health or safety (noting that SQ must give a notice to the Queensland Information Commissioner explaining the extent to which this exemption applies, whether it is a permanent or temporary exemption and, if temporary, which the exemption will cease to apply); and/or
- Is likely to compromise or worsen SQ's cybersecurity or lead to further Data Breaches of SQ – if this exemption applies, SQ will notify the Queensland Information Commissioner explaining the extent to which this exemption applies, when SQ anticipates this exemption will stop applying and how SQ will review the application of this exemption, which must be at least each month for which the exemption applies.

5.6 Stage 6: Post data breach review and remediation

The Privacy Officer is to coordinate and conduct a post incident review with all relevant parties to assess the effectiveness of SQ's response to a Data Breach including, what processes worked well, how issues were handled, and areas for improvement in respect of SQ's management of Data Breaches (including this Policy and any other policies and procedures relied upon in responding to the Data Breach). Tools and steps which may be used to prepare the post-incident review include the following:

- Surveys;
- Immediate debriefs;
- Formal review meetings;
- Process improvement sessions.

The post Data Breach incident review may be conducted by a third party (at SQ's discretion).

As a result of review activities, areas of improvement may be identified relating to people, processes, or technology. The Privacy Officer, in conjunction with Technology Services, will analyse the collected observations and insights to identify potential actions and recommendations to address process and / or safeguard

improvements. A strategy implementing improvements and / or corrective activities may be implemented as a result.

The Privacy Officer will ensure sufficient details of the breach and response steps are recorded in a post incident report and ensure all approved mitigation activities are completed.

6 Record Keeping

SQ documents its management of and responses to actual or suspected Data Breaches, including Eligible Data Breaches, in its Information Risk Registers, Incident Logs, Situation Reports, Evidence Logs and Post Incident Reports as applicable.

As outlined at section 4.6, the Privacy Officer has responsibility for maintaining SQ's Register of Eligible Data Breaches.

The Communications Manager has responsibility for publishing, monitoring and reviewing the currency of public notifications of Data Breaches published to the SQ website.

7 Human rights compatibility

SQ is committed to respecting, protecting, and promoting human rights in accordance with the *Human Rights Act 2019* (HR Act). Under the HR Act, SQ has obligations to act and make decisions in a way that is compatible with human rights, and to give proper consideration to human rights when making decisions. Human rights are not absolute and must be balanced against the rights of other individuals and matters of public importance.

Any delegate making a decision under this Policy must give proper consideration to human rights and whether a decision is compatible with human rights, in compliance with the HR Act.

In deciding to make this Policy, SQ has identified the rights of freedom of expression, privacy and reputation, as being relevant. The Policy does not limit human rights as it promotes the recognised human right of privacy and reputation by facilitating SQ's lawful handling and security of personal information.

8 Related legislation and policies

In addition to SQ's obligations under the IP Act, SQ's response to a Data Breach or other data related incident will also be supported by other policies and procedures maintained by SQ from time to time. This includes:

- Data Breach Response Plan;
- Business Continuity Management Plan (Corporate);
- Crisis Management Plan;
- Cyber Security Incident Response Plan;
- Information Privacy Policy;
- Queensland Privacy Principles Policy.

SQ staff will be required to comply with such internal policies, procedures and processes in the course of their employment, and should consult the internal policies including the Data Breach Response Plan for detailed guidance on how to respond to a Data Breach in accordance with this Policy.

9 Document management

Policy/Procedure owner	Information Management Coordinator
Document category	Policy
Document number	25/17520
Version number	1.0
Effective date	1 July 2025
Last reviewed date	2 July 2025
Last updated date	2 July 2025
Review by date	30 June 2026

10 Revision history

Version	Approved on	Approved by	Amendment category	Changes made
1.0	2 July 2025	Group Executive, Finance and Corporate Services		

11 For more information

For more information on this document, contact SQ's Privacy Officer by email at RTI-Privacy@stadiums.qld.gov.au or phone 07 3008 6100.