Data Breach Policy

Policy

# Purpose

This policy outlines Urban Utilities’ approach to identifying and responding to data breaches.

# Applicability of the Policy

This is an externally-facing policy, required under the *Information Privacy Act 2009* (Qld). This version of this policy takes effect from 1 July 2025.

# Scope

This policy applies to all employees, consultants, contractors and other representatives of Urban Utilities. It also applies to suppliers to Urban Utilities.

# Related Legislation

* *Information Privacy Act 2009* (Qld)
* *Security of Critical Infrastructure Act 2018* (Cth)

# Policy Statement

Urban Utilities is committed to protecting the security of the information that it holds, including personal information. Urban Utilities recognises that implementing robust data breach management processes is essential to managing both security and privacy risks.

Identifying Data Breaches

Urban Utilities has implemented and is continually improving controls to support timely prevention, identification and mitigation of data breaches. These include:

* information security, cyber security and privacy protection processes;
* security and privacy training and awareness for all staff members;
* internal data breach reporting and escalation mechanisms;
* appropriate controls including within supplier agreements;
* internal and external complaints and enquiry processes and
* emergency and incident response plans.

Where a data breach, or suspected breach, is identified, Urban Utilities will take immediate action to contain the breach. Dependent on the nature, source and scale of the data breach, relevant business area teams will be engaged either on an operational or incident response basis to support containment, investigation, mitigation and other response activities, including any notifications that may be required under relevant legislation. Detailed processes and triggers for engagement with business teams are maintained in Urban Utilities’ Mandatory Data Breach Notification Procedure and data breach response plans.

Assessing Data Breaches

If it is identified that the data breach may involve personal information, the breach will be escalated to Urban Utilities’ Privacy Team to determine whether the breach is likely to result in serious harm to an individual and accordingly constitutes an eligible data breach. This process will take a maximum of 30 days. When making this determination, the Privacy Team will consider:

* the kind of personal information accessed, disclosed or lost;
* the sensitivity of the personal information;
* the number of individuals affected by the breach;
* the persons or kinds of persons who obtained or could obtain the personal information as a result of the breach where known;
* the nature of the likely harm;
* security measures including the number of security measures protecting the personal information;
* the time taken to identify the breach and effectively mitigate it; and
* any other relevant circumstances.

The Privacy Team will record the decision-making process and the outcome involved in each data breach assessment and capture root cause analysis and corrective actions information to support continuous improvement and data breach prevention activities.

Notifying Data Breaches

If Urban Utilities determines that an eligible data breach has occurred, it will notify the Office of the Information Commissioner (OIC) and individuals whose personal information was disclosed, accessed or lost and any other affected individuals as soon as practicable, unless an exemption applies under the *Information Privacy Act 2009*. These exemptions include scenarios where:

* notification is likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal;
* the eligible data breach has affected more than one agency and the other agency is providing notification;
* remedial action has been taken to mitigate the harm before any serious harm has resulted and, as a result of the action, serious harm is no longer likely to result;
* notification would require non-compliance with another Act which prohibits or regulates the use or disclosure of information;
* notification would create a serious risk of harm to an individual’s health or safety; **or**
* notification is likely to compromise cybersecurity or lead to further data breaches.

Where no exemption applies, but it is not practical to notify individuals directly, Urban Utilities will notify the OIC and make information, other than information that would prejudice Urban Utilities’ functions, available about the breach on its website for 12 months.

If Urban Utilities determines that a data breach is not an eligible data breach because it is not likely to result in serious harm to an individual, it will still endeavour to notify individuals of data breaches involving their personal information. This notification will be provided where Urban Utilities considers it is practical and reasonable to do so and notification is unlikely to create risk for the security of Urban Utilities’ information and systems or an individual’s safety.

Individuals may make a privacy complaint in relation to a data breach by contacting Urban Utilities via email to [UrbanUtilities.information@urbanutilities.com.au](mailto:UrbanUtilities.information@urbanutilities.com.au) or via mail to:

Urban Utilities

Attention RTI and Privacy Team

GPO Box 2765

Brisbane QLD 4001

Urban Utilities will respond within 45 business days after the complaint is received.

Recording Data Breaches

Urban Utilities will maintain a data breach register to record information for each eligible data breach, including details of any notifications to individuals or the OIC, any applicable exemptions, steps it has taken to contain and mitigate the breach and actions taken to prevent future breaches of a similar kind occurring.

# Definitions

|  |  |
| --- | --- |
| **Control** | A prevention, detection or response measure to reduce the likelihood or impact of a data breach. |
| **Data breach** | Unauthorised access to or disclosure of information orloss of information in circumstances where unauthorised access or disclosure is likely to occur. |
| **Eligible data breach** | A data breach which (a) involves personal information and (b) is likely to result in serious harm to an individual to whom the personal information relates. |
| **Personal information** | Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion (a) whether the information or opinion is true or not and (b) whether the information or opinion is recorded in a material form or not. |

# Related Documents

Internal Documents

* POL29 Information Privacy Policy
* POL54 Information and Cyber Security Policy
* PRO763 Privacy and Right to Information Management Framework
* Mandatory Data Breach Scheme Procedure

External Documents

* Mandatory Notification of Data Breach Guidelines, Office of the Information Commissioner

# Review Date

This policy will be reviewed every 2 years or in accordance with changes to relevant legislation or business objectives.

# Authorising Officer

Urban Utilities Board