Data Breach Notification Policy

Version 1

Contents

1. Objective

Cloudoffis Pty Ltd is legally obliged to comply with the new PRIVACY AMENDMENT (Notifiable Data Breaches) Act 2017 (Cth) and other applicable privacy laws and obligations. We aim to work together to minimize the impact of data breaches and protect our client's interests.

Information/Data is one of the most critical assets, and it is a mandatory responsibility for Cloudoffis Pty Ltd and its Clients/Users to ensure the security of this information.

The sole purpose of this policy is to ensure a standard approach is in place in the event of an information/data breach.

2. Scope

The Data Breach Notification policy applies to all Cloudoffis employees, users, service providers, contractors, customers, and any third parties that access, use, store and process information at Cloudoffis.

The policy is authorized by the senior management of Cloudoffis Pty Ltd.

3. Policy Statement

As per Cloudoffis' 'Notifiable Data Breaches' policy, all stakeholders should strictly adhere to the following plan in the event of any information or data breach. Identification and Classification

- Containment & Recovery
- Risk Assessment
- Notification of Breach
- Evaluation & Response

4. Breach Management Plan

4.1 Identification & Classification

- All users and customers must notify the Cloudoffis team in case of any information/data breach occurrence.
- The above would equip the Cloudoffis team to deal with the incidents in the most appropriate manner.
- Client/Users should work with the Cloudoffis Team in investigating and assessing the incident to the eligibility of the Data Breach incident
- Details of the breach should be accurately recorded with the following details
    - Data and time when the breach occurred
    - Data and time when the breach was detected
    - Description of the breach
    - Details of any systems involved
    - Additional details such as; Error Messages, Logs, etc.
    - Recommended steps (initial) to be taken
- Concerning the policy; An Eligible Data Breach may be defined as an intentional/unintentional release of Cloudoffis' or its client's, personal information/data to unauthorized person(s), either via

an accidental or deliberate disclosure resulting in Unauthorized access, loss or theft of the information/data

4.2 Containment and Recovery

It involves limiting the scope and impact of a breach of information/data. If a breach occurs, Cloudoffis and its clients/users should:

- Work together and decide who would take the lead in investigating the breach and ensure that the appropriate resources and details are made available for investigation
- Establish whom to be made aware of the breach (should be informed of)
- Identify whether anything can be done to recover the losses and/ limit the damage, the breach can cause
- Work together to contain and mitigate the eligible data breach, protect affected client/users, and protect the information from further breaches
- Work together, investigate, decide and implement appropriate remedial and mitigation steps

4.3 Risk Assessment

While assessing the risks (from breach), one must consider their potential consequences and substantiality. The following should be considered while assessing the risk:

- What type of information/data is involved?
- How sensitive the information/data is?
- What could the information/data tell third parties?
- How many are (and how much is) affected by the breach?

4.4 Breach Notification

- Cloudoffis has and established contact channels to inform or communicate 'potential data breaches'. A client can also use the designated contact channel to report breaches (incidents)
- Any Client/User coming across the situation of a potential data breach (or the one that already happened) should immediately contact the Cloudoffis team
- Client/Users should cooperate and provide all assistance to the Cloudoffis team to ensure compliance with its legislative and contractual obligations (Defined as per the Eligible Data Breach).
- If Cloudoffis compliance prevents its clients/users from complying with any applicable laws, the clients/users should notify the Cloudoffis team.

4.5 Evaluation and Response

- After any information/data breach incident, a thorough review of the incident should happen
- The incident should be documented with all the details and samples, along with the cause of the data breach. The document should also include a prevention plan which will help to prevent it from occurring again in the future
- The purpose of the review is to ensure that the remediation actions were appropriate and that the areas of improvement will be identified.

- Any recommended change of policies and procedures should be documented and implemented immediately after that and shall be included in future audits.

5. Cloudoffis Contact Information

- **Email Address:** support@cloudoffis.com.au
- **Office Phone Number:** 1300 979 457

6. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Data Breach Notification Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version created	11 Jun, 2024
1	New Policy version Created	11 Jun, 2024