Axeten Data Breach Policy

February 2024

Introduction

Axeten (hereafter also referred to as “we”) collects, holds and processes data, a valuable asset that needs to be suitably protected.
Axeten makes every effort to protect the confidentiality, integrity and availability of personal information of its stakeholders. We employ security measures consistent with best practice to protect against unauthorised access to personally identifiable information. For further information on our security plan, please see our Security Policy.

Scope

This policy sets out the procedures to be followed to ensure that a consistent and effective approach is in place to avoid a data breach that could compromise security.
The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definition

A data breach is an incident (confirmed or suspected) in which protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data relating to personal information, either accidentally or deliberately, and has caused or has the potential to cause damage to the information, assets and/or reputation of Axeten.

Types of Data Breach (confirmed or suspected)

An incident includes but is not limited to the following:-

- theft of data or equipment on which such data is stored, and;
- equipment failure, and;
- unauthorised access to confidential information, and;
- unauthorised disclosure of confidential information, and;
- cyber attack (generally known as a hacking attack), and;
- unforeseen circumstances such as a fire or a flood, and;

• human error.

Data Breach Management Plan

Axeten has in place a breach management plan to follow should such an incident occur. There are five elements to our breach management plan:-

1. Identification and Classification

In the event of a breach, an initial assessment would be made to establish the severity of the breach. Details of the breach would be recorded accurately, including the date and time the breach occurred, the date and time it was detected, who reported the breach, and a description of the breach.

2. Containment and Recovery

Should a breach occur, where data is deleted, the IT department shall restore it from backup, to mitigate against loss. The data breach shall be contained after identification and classification through immediate and effective action by our IT Department. For example, the following actions might be taken:-

- shut down the system that was breached,
- block access from the unauthorised person,
- revoke or change the account privileges,
- stop the unauthorised practice and recover any records.

3. Assessment of Risk

Assessment of risk is the responsibility of the data controller. In the event of a breach, we would not be assessing risk, but we would be transparent in the notification to the data controller.

4. Notification of the Data Controller

Data controllers shall be notified in case of breach. Notification shall include a description of how and when the breach occurred, and the data involved.

5. Post Breach Evaluation and Response

Once an initial incident is contained, we would carry out a full review of the causes of the breach, the effectiveness of the response and what changes to systems, policies and procedures should be undertaken.
The purpose of this review is to ensure that the steps taken during the incident were appropriate and that a breach would not occur again.
All data security breaches would be logged on Axeten servers to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

Policy Update

This policy shall be reviewed and updated annually, to ensure that any changes to the security and data breach practices of Axeten are properly reflected in the policy. Please check this policy regularly.

References

To read or download our compliance documents, please go to https://www.axeten.com/documents

- Axeten Processing Privacy Policy
- Axeten Training Privacy Policy
- Axeten Security Policy
- Axeten Data Protection Compliance Statement
- Framework Data Processing Agreement
- Axeten Modern Slavery Policy
- Axeten Equality and Diversity Policy

//end