# Introduction

This Policy has been created to describe the approach taken by the ORGANISATION NAME to ensure that data breaches are identified and responded to quickly and effectively.

The ORGANISATION NAME is committed to safeguarding the confidentiality, integrity and availability of personal data and information assets.

This policy is made available to all who work for or on behalf of the ORGANISATION NAME and to interested parties upon request.

# Scope

All employees, contractors and third parties who have a role in delivering services or accessing information controlled / owned by the ORGANISATION NAME are included within the scope of this policy.

# Responsibilities

All users and owners of information assets must follow this procedure for reporting information security events, incidents, and weaknesses. The JOB TITLE is responsible for logging and managing reported incidents and the response to those incidents. The JOB TITLE will document the steps taken to identify the root cause of an incident and is then further responsible for applying corrective action to close out the report.

It is also the responsibility of the JOB TITLE to ensure that a log is maintained of all incidents that occur, no matter their nature, and to provide a summary report to senior management on a periodic basis, the summary must include the number, frequency and types of incidents occurring.

Employees, visitors, contractors and other third parties are expected to report security incidents which affect ORGANISATION NAME as soon as they are noticed.

Where a security incident or potential incident has been identified by a customer or other third party, it is the responsibility of the relationship owner to report the case to the JOB TITLE.

##### Definitions

Security Event Is a minor happening that could lead to a security incident. (Example, someone wrote down their password and lost it, this could lead to someone finding it and gaining unauthorised access to a system or services).

Security Incident Is where a weakness or event has been exploited and an incident has occurred (Example: Someone wrote down their password and lost it, a malicious outsider found it and gained access to the financial payment system).

Data Breach A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Root cause The root cause is the underlying issue as to why an incident occurred.

Containment Action taken to ensure the immediate containment of a weakness, event, or incident.

Correction Actions taken to reduce the risk of a weakness, event or incident recurring.

##### Procedure

Information security weaknesses, events and incidents are reported immediately as they are seen or experienced, to the JOB TITLE. Reports can be made via email, phone call or in person. In the absence of the DPO, ORGANISATION NAME Directors have authority to log and manage the report.

It is possible that users may not be allowed to continue working on an affected system until an identified possible weakness or security event has been resolved and they are authorised to resume working.

##### Responding to Information Security Events, Incidents & Breaches

All information / data security events and incidents are, at once upon receipt, logged within the Data Breach Log and assessed and categorised as per their criticality:

* Security Event
* Security Incident
* Data Breach

When there are multiple event reports in each category, The JOB TITLE prioritises responses in the light of the criticality to the business.

The JOB TITLE will decide if immediate containment of the incident / event is required and will design actions to prevent the incident / event from spreading or getting worse. This can involve:

* Isolation of a system, network, application, or device
* Cordoning off a physical area
* Preventing access (electronic or physical) until the incident is contained
* Contacting emergency services to perform containment

Once the incident is contained, the JOB TITLE will perform root cause analysis to identify the cause of the event / incident. Corrective action will then be applied to address the root cause and to prevent the event / incident from recurring. The JOB TITLE will perform an assessment to identify if personal data has been breached, and where it has, will use the flow chart at the end of this document to ensure that any reports to the Information Commissioner are made.

The JOB TITLE is responsible for closing out the incident.

This includes:

* any reports to external authorities, such as police, Information Commissioners Office. Where the media is concerned communication must be dealt with via approved ORGANISATION NAME persons.
* initiating disciplinary action as appropriate by dealing with it through the HR process,
* planning and implementing preventative action to avoid any further recurrence,
* initiating any action for compensation from software, service or outsource suppliers by referring the incident to the appropriate manager,
* communicating with those affected by or involved in the incident about returning to normal working and any other issues.

The JOB TITLE provides reports to Senior Management with a summary of the incident, which will include how the ORGANISATION NAME could have responded earlier or more effectively, or preventative action that might have been taken in advance of the incident and the effectiveness of the containment and corrective actions, the contingency plans and how the incident was closed out.

All information gathered during the response to an information security incident is potentially evidence to be used in a disciplinary, criminal, or civil action. Care is taken to preserve the evidence in such circumstances.

In case of a serious breach of security, a breach concerning personal data or a criminal act where evidence must be preserved, the following must be adhered to:

* Evidence should be collected and preserved as soon as possible.
* Ensure staff cannot access the incident site.
* Statements should be taken from those involved (if applicable)
* Photographs should be taken of the incident and any other contributing factors.
	+ Where criminal activity is suspected, the police should be contacted immediately. This is the responsibility of the JOB TITLE only who will seek council with the Senior Management prior to reporting.

Employees are not permitted to make reports to law enforcement agencies without the explicit consent of the senior management team.

Incident reports are reviewed as part of the management review process to ensure that the ORGANISATION NAME learns from the incidents.

##### Reporting to Authorities

If a breach of security which affects personal data is identified, it must be swiftly reported to the JOB TITLE so that an assessment can be made as to whether the incident needs to be reported to the Information Commissioners Office (ICO), and potentially affected data subjects within 72 hours.

The below flow chart shows the actions that shall be taken if a breach concerning personal data is identified:

Any employee, volunteer / contractor or third - party reports event / incident / breach

Start

YES

NO

Does the incident involve personal data?

YES

Is the data encrypted?

YES

NO

Is the data sensitive or large scale?

NO

JOB TITLE - Ensure to manage the incident as per the requirements of this procedure. Log incident details, root cause & corrective action to the Incident log

JOB TITLE - conduct Root Cause Analysis and identify the cause of the issue – apply corrective action to prevent the issue recurring

JOB TITLE to Log incident within the incident log and assess to place in the following categories

* Event
* Weakness
* Incident

JOB TITLE - Apply an immediate short term containment action to prevent the issue becoming worse or spreading

JOB TITLE – Close Report

JOB TITLE – Communicate ICO action to Chief Executive & Finance Director

JOB TITLE – Update breach report with details of report and communications from ICO

JOB TITLE - Report to the Information Commissioners Office (ICO) via the online reporting tool.

Contact affected data subjects and explain the breach and to what extent they are affected

SENIOR MANAGEMENT - Review breach report details and provide authorisation to report

JOB TITLE - Inform Senior Management of the need to report to the ICO, provide full details of breach and seek authorisation to report.