SECURITY INCIDENT REPORTING POLICY

Policy Statement

The management of security incidents is central to the ISO 27001 Information Security Management System (ISMS). It is essential that incidents are not only investigated but that corrective action is taken and the results are monitored. Similarly, potential incidents should also be documented and preventive action taken.

The purpose of this Policy is to protect the confidentiality, integrity and availability of the Organisation's information by ensuring that:

1. Security incidents are reported and resolved in the minimum amount of time
2. Potential security incidents are prevented from happening in the first place
3. The Organisations's security is continually improved by the application of corrective and preventive action.

Scope

The scope of this policy applies to:

1. The Organisation's personnel, temporary staff, contractors and service providers utilising the Organisation's information system resources from any location
2. All Organisational premises and the physical security pertaining to them
3. Information system resources, including data networks, LAN servers and personal computers (standalone or network-enabled) located at the Organisation's premises, where these systems are under the jurisdiction and / or ownership of the Organisation, and any personal computers and / or servers authorised to access the Organisation's data networks. Third parties shall also adhere to this Policy
4. Remote access connections used to do work on behalf of the Organisation, including reading or sending e-mail and viewing intranet web resources.

Objectives

1. To protect the integrity and availability of the Organisation's information by ensuring that security incidents, or potential incidents, are identified, brought to the attention of the Information Security Manager and dealt with in a manner appropriate to the urgency and impact of the breach.
2. To define the reporting procedures to be followed in the event of a security incident taking place, or a potential security incident being noted.

Principles

1. All security incidents must be logged and resolved within the minimum amount of time.
2. Potential security incidents should be prevented from occurring in the first place.
3. All incidents must be resolved by taking appropriate corrective and preventive action, thereby ensuring no recurrence of the incident.

Responsibilities

1. The Head of Operations (ISMS Manager) is responsible for ensuring that security breaches and weaknesses (both regarded as a security incident) are identified and dealt with in accordance with this Policy.

2. All of the Organisation's employees are responsible for making a vigilant and responsible contribution to the security of the Organisation's information resources. Deliberate failure to report a known security breach or weakness may lead to disciplinary action under the Organisation's disciplinary policy.

Definitions

1. A security breach is the actual occurrence of an event which led, or could lead, to a compromise of the confidentiality, integrity or availability of the Organisation's information resources. Examples include:

    - A burglary
    - A hacker gaining access to one or more of the Organisation's servers
    - Loss of confidential papers
    - Loss of a mobile device (e.g. a smart phone, laptop or tablet computer) containing confidential or sensitive information.

2. A security weakness is a set of circumstances which provides the potential for occurrence of a security breach. Examples include:

    - Staff being permitted to copy data on to unencrypted memory sticks and take them home
    - Incorrect client site data being loaded on the Internet for that client
    - Unencrypted web access to websites containing personal data.

Measures to be taken

1. Security breaches and weaknesses are to be reported immediately to the Reportee's Line Manager.

2. In conjunction with the Line Manager, a Management Information Report of the incident is immediately produced (please see appendix for template).

3. The Management Information Report is sent immediately to the Information Security Manager.

4. The Head of Operations (ISMS Manager) takes action to address the security breach or weakness in a manner appropriate to its urgency and impact, in conjunction with the Reportee's Line Manager.

5. In the case of a security breach, the corrective action taken is documented on the (document name) and the situation monitored until assurance is achieved that the breach has been closed.

6. In the case of a security weakness, the preventive action taken is documented on the (document name).

7. Information Security Breach Reports are reviewed periodically at an appropriate level of management and signed off when the issue is closed.

Where data has been compromised in terms of its confidentiality, integrity or availability, the Information Security Manager consults with other senior management of the Organisation to ensure that affected parties are identified and appropriately informed. N.B. There is an obligation on the controller to report personal data breaches to the supervisory authority (usually the Information Commissioner's Office) where the breach is likely to adversely affect the personal data or privacy of the data subject.

User awareness

- This Policy will be drawn to the attention of all Organisational staff.

Compliance

- IS0 27002: Clauses 16.1.1 (Responsibilities and Procedures) and 16.1.2 (Reporting Information Security Events).

Responsibility for implementation

- ISMS Manager

Policy Signoff

Date of Issue:	27/10/2020
Date of Next Review:	15/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	FINAL
2.0	27/10/2020	Jo Holloway	Update of dates