**Incident Management Procedure**

**Doc A16**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 Company Incident Management Procedure 3

1.1 Scope 3

1.2 Definitions 3

1.3 Responsibilities 3

2 Procedure 4

2.1 Reporting Information Security Events and Incidents 4

2.2 Collection of Evidence 4

3 Document Control and Approval 6

3.1 Distribution 6

3.2 Version Information 6

# Company Incident Management Procedure

## Scope

This procedure defines the process for the management of information security incidents, including communication on security events.

## Definitions

         ‘**Events**’ are occurrences that, after analysis, have no or very minor importance for Information Security;

         ‘**Incidents**’ are occurrences of events (or series of events) that have a significant probability of compromising Company’s Information Security;

## Responsibilities

The Information Security Manager is responsible for this procedure.

Executives, Directors and Managers are responsible for ensuring this procedure is understood and complied with within the organization.

Staff are responsible for reporting information security incidents and events as necessary under this procedure.

The Information Security Manager is responsible for logging and following up on reported incidents and events.

All Staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Questions regarding the content or application of this policy should be directed to your line manager.

Visitors who have physical access to the Company’s offices are also required to comply with this procedure and should inform their host to report events.

Where Staff work in an office space provided by a customer, supplier or other 3rd party, Staff are also expected to follow the security policies and procedures provided by the 3rd party.

# Procedure

## Reporting Information Security Events and Incidents

The following are typical incidents that fall within the scope of this procedure:

* Breach of Security Policy
* Breach of physical security
* Loss or theft of property
* Breach of information security
* Data/information missing, lost or incorrect

Information Security events and incidents must be raised in the ticket management system (*URL of ticket submission page*)  via the portal (*URL of employee portal*) or by email (*email@ofsecurityteam.com*) as soon as they are seen or experienced.

The Service Desk ensures that the appropriate action is taken and recorded in the Ticketing System.

When there are multiple events reported, the Information Security Manager prioritizes responses in the light of the criticality of the business systems and information assets at risk and the danger of further compromise to Wacky Widget’s Information Security.

If an incident involves a customer owned asset, or production application. Once the incident is contained, and the required corrective action is completed, the Information Security Manager will create a report for the Chief Technology Officer with a summary of the incident, where necessary identifying the cause of the incident and analyzing its progress.

The report will identify how Wacky Widget could have responded earlier or more effectively, or preventative action that might have been taken in advance of the incident, the effectiveness of the containment and corrective actions and the contingency plans and how the incident was closed out.

The Information Security Manager is responsible for closing out the incident. This includes: -

* Working with Legal on reporting to external authorities as required;
* Initiating disciplinary action (with input from the relevant line manager as appropriate);
* Planning and implementing preventative action to avoid any further recurrence;
* Initiating any action for compensation from software, service or outsource suppliers by communicating with those affected by or involved in the incident about returning to normal working and any other issues.

Relevant Incident reports are reviewed as part of the management review process to ensure that Wacky Widget understands the root cause and learns from the incidents.

## Collection of Evidence

All information gathered during the course of responding 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 all information security incidents, irrespective of whether or not a follow-up action against a person or organization involves legal action (either civil or criminal), evidence is collected, retained and presented where needed.

Where the likelihood of legal, civil or criminal action is established early in the incident response process, the police or lawyers are involved as early as possible and their guidance is sought and followed in respect of evidence collection and retention. If the event, or the possible action, spans organizational or geographic boundaries, the Wacky Widget legal team must be consulted to ensure that evidence can be collected and how it should be collected. External advisers or third parties are subject to NDA agreements.

Users may not be allowed to continue working on an affected system until an identified possible Information Security event or incident has been resolved and they are authorized to resume working by the Information Security Manager.

# Document Control and Approval

The Risk and Compliance Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff and is the published version.

This document was approved by Chief Technology Officer and is issued on a version controlled basis.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |