[Insert Company Logo Here]

Information Security Incident Response Procedure

Document Classification	[Insert Classification]
Document Reference	ISMS-Doc-A16-2
Version	1
Dated	[Insert Date]
Document Author	[Insert Name]
Document Owner	[Insert Name/Role]

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Contents

List of Tables

1 Introduction

This document is intended to be used when an incident of some kind has occurred that affects the information security of [Organization Name]. It is intended to ensure a quick, effective and orderly response to information security incidents.

The procedures set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding the actions to take.

However, it is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The objectives of this incident response procedure are to:

- Provide a concise overview of how [Organization Name] will respond to an incident affecting its information security
- Set out who will respond to an incident and their roles and responsibilities
- Describe the facilities that are in place to help with the management of the incident
- Define how decisions will be taken regarding our response to an incident
- Explain how communication within the organization and with external parties will be handled
- Provide contact details for key people and external agencies
- Define what will happen once the incident is resolved, and the responders are stood down

All members of staff named in this document will be given a copy which they must have available when required.

Contact details will be checked and updated at least three times a year. Changes to contact or other relevant details that occur outside of these scheduled checks should be sent to information.security@organization.com as soon as possible after the change has occurred.

All personal information collected as part of the incident response procedure and contained in this document will be used purely for the purposes of information security incident management and is subject to relevant data protection legislation.