**Appendix 1 – Incident Response Plan**

\*\* FREE PREVIEW VERSION \*\*

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 25/08/2010 | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of contents

[1. Purpose, scope and users 3](#_Toc325044647)

[2. Authorisations and responsibilities in incident response 3](#_Toc325044648)

[3. Communication 3](#_Toc325044649)

[4. Procedures for disruptive incidents 4](#_Toc325044650)

[4.1. Managing a disruptive incident 4](#_Toc325044651)

[4.1.1. Obligation of every employee to report incidents 4](#_Toc325044652)

[4.1.2. Disruptive incident handling 4](#_Toc325044653)

[4.1.3. Crisis Manager 5](#_Toc325044654)

[4.2. Containing and eradicating an incident 5](#_Toc325044655)

[4.2.1. Evacuation of the building (regardless of incident type) 5](#_Toc325044656)

[4.2.2. Fire 6](#_Toc325044657)

[4.2.3. Interruption of power supply 6](#_Toc325044658)

[4.2.4. Earthquake 6](#_Toc325044659)

[4.2.5. Threat letter 7](#_Toc325044660)

[4.2.6. Threat call / bomb threat 7](#_Toc325044661)

[4.2.7. Telecommunications failure 8](#_Toc325044662)

[4.2.8. Information system failure 8](#_Toc325044663)

[4.2.9. Malicious code attack 8](#_Toc325044664)

[4.2.10. Violation of internal or external rules 9](#_Toc325044665)

[5. Managing records kept on the basis of this document 9](#_Toc325044666)

[6. Validity and document management 9](#_Toc325044667)

# Purpose, scope and users

The purpose of this Plan is to ensure the protection of health and safety of people in the case of disaster or other incident, and to contain the incident. The objective is to reduce damage to the business to the smallest possible extent.

This Plan is applied to all major incidents threatening to disrupt any critical activity within ISMS [BCMS] scope for a period longer than the recovery point objective for each individual activity (further in text: disruptive incidents).

Users of this document are all employees of [organization name].

# Authorisations and responsibilities in incident response

|  |  |
| --- | --- |
| ***Role in recovery / job title*** | ***Authorisations and responsibilities*** |
| ... | ... |

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: http://www.iso27001standard.com/en/documentation/Appendix-1-Incident-Response-Plan