***Contents***

[**1. Introduction 2**](#_Toc431889575)

[**2. Information Security Processes 4**](#_Toc431889576)

[**3. Emergency Response 5**](#_Toc431889577)

[**4. Personnel 7**](#_Toc431889578)

[**5. Information Systems and Communications 10**](#_Toc431889579)

[**6. Financial and Legal 13**](#_Toc431889580)

[**Document Owner and Approval 15**](#_Toc431889581)

# Introduction

* 1. The purpose of this plan is to set out the steps *{OrganisationName}* will take to ensure information security during and after a **disaster,** whether minor, moderate or major, i.e. the loss of a significant part of the function of the ISMS for more than a few hours. Causes are typically in line with business continuity threats. The *{EmergencyResponseTeams}* will follow this plan, and the management team are committed to it.
  2. Following a disaster, the typical response **lifecycle** would be:
* Emergency response to assess level of damage, decide whether to invoke the plan and at what level, to notify Employees/Staff etc.
* Provision of an emergency level of service
* Restoration of key controls
* Recovery to business as normal.
  1. **Target times** have been established for the above stages:
* to be completed within two business hours of the disaster
* within six business hours of the disaster
* within two days of the disaster
* within five days of the disaster.
  1. The **key resources** of *{OrganisationName}* are:

Employees/Staff - provision of services is dependent on the knowledge and skills of existing Employees/Staff.

*Premises* – *[identify the sites that are covered by this plan].*

*[Telephone handling] team* - handling visitors, post and incoming calls.

*Telephony* - the telephone lines, *[telephone infrastructure detail]*.

*Information Technology* - the data, software, hardware - file servers, PCs, printers etc., structured cabling for data and telephony, LAN equipment, WAN equipment.

*Paper records* and filing systems.

*Services -* Power, heating, lighting, water, etc.

* 1. The strategic issues affecting the development of this plan are:

[*Set out here the key issues that affect the structure of your business continuity plan – what alternative sites and facilities are available, which services you need to have working within how long, what the key dependencies on {OrganisationName} are, etc. – the business continuity risk assessment (*[*ISMS-C DOC 17*](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_17.docm)*) is a key input here*].

* + 1. Alternative sites; business continuity sites; use of a disaster recovery service.
    2. The key need immediately following disaster is what, and how will it be handled? I.e. what services have to be restored first, and how quickly does it have to happen?
    3. What additional risk issues might there be around telecommunications and data links?
    4. How long can be allowed to restore operations completely, what limiting factors are there, and what other issues have to be taken into account?
    5. How will Employees/Staff continue working, what will they do, what records will they maintain? Use of wireless laptops, PDAs, mobile phones could be paramount here – with security implications.
    6. Storage of records and backup procedures (fireproof safes, offsite storage, how to access?)
    7. What are the repercussions of a disaster – press, customers, suppliers, others?
  1. This plan will be maintained in accordance with [ISMS-C DOC 17](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_17.docm)*.*
  2. [*How is this plan to be made available to* Employees/Staff*, to management and to members of the {EmergencyResponseTeams} – in the event of an emergency, where the corporate systems are all down?*]

# Information Security Processes

* 1. Perimeter controls

Theperimeter controlsof *{OrganisationName}* and the persons responsible for them are**:**

[*List all controls used to secure the information security perimeter, with a brief description of them. Also identify the {Manager} responsible for each of them. Then identify, for each of the controls, those information assets that are part of them, cross referencing to* [*ISMS-C DOC 8*](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_8.docm)*, and identify their [owners] – a hyperlinked matrix, or database, is probably ideal for this, as long as you can access it in case of disaster.*].

* + 1. Alternates [*alternate managers, who can take over responsibility in case a line manager is out of action*] are identified in Section 4.3.
  1. Internal controls

The internal controls of *{OrganisationName}* (the ones that secure information within *{OrganisationName}*), the persons responsible for them are [*e.g. Finance, Marketing, Production, HR, Training, Logistics, and the information assets that are involved in them are ] [This section needs also to deal with disasters or service interruptions at organisations to which critical services have been outsourced.*]

* 1. Priorities

Following a disaster, the immediate information security priorities are (in descending order):

* + 1. [*Set out, in descending priority, your requirements for achieving continuity, identifying which controls have to be restored, in what order and why.*]

# Emergency Response

* 1. Emergency responses are conducted in line with information security incident management policies and processes ([ISMS-C DOC 16](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_16.docm)).
  2. *{EmergencyResponseTeams}* (ERT)

The team comprises those Employees/Staff listed on the Emergency Team Contact Card [*If you go this route, you will have small cards made up with the names and emergency contact details of the 3-4 members of the {EmergencyResponseTeams} listed, and these cards will go to all* Employees/Staff *so that, in the event of an emergency, they have someone to contact.*]

Contact details are *[where?]*; all staff are issued with a card containing *{EmergencyResponseTeams}* contact details, to be used in the event of a disaster.

The responsibilities of the *{EmergencyResponseTeams}* are to:

* respond immediately to a potential information security continuity threat, assess the extent of the threat and its impact on information security,
* decide which elements of the Information Security Continuity Plan should be invoked,
* establish and manage an Information Security Recovery Team to return to normal operation,
* ensure Employees/Staff are notified and allocate responsibilities and activities as required.

**Appendix 1**

**Emergency alert, escalation and ISCP invocation procedure**

This procedure applies at all *{OrganisationName}*’s sites. The *[identified role]* is responsible for invoking the BCP in respect of any of the disasters identified in this plan as well as in the event of any other occurrence that affects *{OrganisationName}*’s capability to perform normally.

# Personnel

* 1. Alternates

Key Employees/Staff have an alternate nominated who has the knowledge and ability to be able to deputise, at least on a temporary basis, should that member of staff be unavailable. *[Second alternates may be required for some roles.]*

**Role Holder Alternate**

*[List all the roles identified in 2.1 and 2.2 above, name the individual who holds the role, and identify alternates who could take on the responsibility.]*

* 1. Calling Tree

A calling tree mechanism has been devised to share the work of ensuring that all staff are notified of the information security continuity event, rippling down from the *{EmergencyResponseTeams}* to the *[senior managers]* and then to the rest of the Employees/Staff. The person discovering the information security continuity event calls a member of the *{EmergencyResponseTeams}*, trying in the order listed on their disaster card; if no *{EmergencyResponseTeams}* member is available then alternates are tried.

The calling tree and contact numbers for key Employees/Staff are shown at Appendix 5 of this section.

**Appendix 3**

**Calling Tree**

[*Create as many of these calling trees as you need to set out clearly who has to contact who, and in what order*]

**ERT Leader (or first member of ERT notified)**

Remaining members of ERT

Who?

Who?

**Next member of ERT**

Who?

**Appendix 4**

**In Confidence - EMERGENCY USE ONLY**

**Staff contact numbers**

**Site 1 Main line**

| **Name** | **Role** | **Home number** | **Mobile number** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Site 2 Main line**

| **Name** | **Role** | **Home number** | **Mobile number** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Site 3 Main line**

| **Name** | **Role** | **Home number** | **Mobile number** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

# Information Systems and Communications

* 1. Paper Records

Some important information exists solely in paper form; this includes:

* personnel records
* some financial records
* signed partner and supplier contracts
* some client information.

Key personnel, financial and legal documents are kept in a fire-proof cabinet [*which is precisely where?]* and certain key documents may be kept offsite *[what and where?*].

* 1. Computer system
     1. Backup arrangements *[describe what is backed up, to where, and who to contact. If there is more than one arrangement (i.e. one per site), describe them all]*.
     2. Describe what your emergency computer arrangements are, both for how you restore information security and for how you recover. If this involves buying computing or related equipment, you need to set out here where it comes from, what type of equipment needs to be purchased, what software, etc.]
     3. The relative priorities for restoration of the computer applications will be determined by the *{EmergencyResponseTeams}* but is likely to be:

*[Set out, in terms of your service restoration priorities, what the order of computer system restoration should be]*.

* + 1. The planned approach is:

*[Set out, step by step, what you will do in order to achieve that restoration requirement]*

There are full instructions for the restore operation in the IT Department Working Instructions *[which are available where and how?]*.

* + 1. The timescale *[describe the expected timescale for each of the stages, so that you can easily identify where things are going off track]*.
    2. The use of existing home based/mobile computer equipment during restoration may be of some limited help in maintaining services. *{Manager}* have [*PDAs*] which contain details of key contacts and meetings.
  1. Software

An analysis of the relative importance and difficulty of securely re-installing the key software products in use at *{OrganisationName}*, together with contact details is contained in the following table. [*This table should link back to your software asset log (ISMS-C REC 8.1.1) and you should ensure you have identified how you will restore each type of software if you have to rebuild.*]

| **Software** | **Analysis – importance and options** | **Contact** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Wide Area Network/WLAN/LANs
     1. [*Set out relative priorities for restoration, options in the short term, and the necessary technical specifications (a detailed network map, with hardware specifications, can be helpful here) and contact details to enable you to restore this service.*]
     2. The network comprises the following elements:

[]

* + 1. Contact details are:

[]

* 1. Telephony
     1. [*Repeat the exercise with telephony, looking at fixed links as well as at mobile phones.*]
     2. [*Determine what will happen when someone phones a site that is out of action – i.e. what automatic diverting routines do you have?*]
     3. For problems affecting the switchboards of handsets, contact [*provide details for telephone switches, handsets, etc.*].
     4. In the event of an electrical power failure:

[*Set out, for each of the sites, what will happen if there is an electrical power failure, at the site or at the premises of a service (e.g. telecoms) supplier, and how you will deal with this. You should include analogue phone services, diversion services and so on in your plans. This will need to include all the contact details necessary to deal with this issue*.]

**Appendix 1**

**IT, Telephony, Post contact list**

| **Category** | **Company** | **Tel** | **Contact** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Financial and Legal

* 1. An assessment shall be made by the emergency response team of the impact on the financial affairs of *{OrganisationName}*. The assessment should include:
* toss of confidentiality, integrity or availability of information
* loss of financial documents
* loss of revenue
* theft of cheque books ,etc.
* loss of cash
  1. Company credit cards could be used to pay for supplies and services required following an information security event.
  2. [*Bank account details, bank manager, contact details.*]
  3. The *{EmergencyResponseTeams}* will decide whether there may be legal actions resulting from the disaster; in particular, the possibility of claims by or against *{OrganisationName}*. [*Provide details of commercial lawyers who would handle claims on behalf of {OrganisationName}.*]
  4. If legal actions are possible, then the *{BoardDirectors}* should be advised:

**Insurance, financial, legal contacts list**

| **Type** | **Company** | **Tel** | **Contact** | **Role** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Document Owner and Approval

The *{InfoSecManager}* 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/specified]* members of staff on the *[corporate intranet]* and is published *[ ]*.

This procedure was approved by the *{ChiefInfoSecOfficer}* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |