

**Business Continuity Plan**

**<NGO>**

**Ver.1.0**

**<Date>**



**Copyright**

This document and the accompanying templates were prepared by Tournis Consulting LP and the precious contribution of CPMS and emcra GmbH as one of the deliverables of the CASSANDRA Project that has been funded with support from the European Commission.

This document is free to be downloaded and used for improving resilience of any organisation, under the terms of Erasmus+ programme.

This document is subject to the licence:

by-nd

**Creative Commons Attribution NoDerivatives Version 4.0, by CASSANDRA-Project** (CC-BY-ND, <https://creativecommons.org/licenses/by-nd/4.0/legalcode>):

CC-BY-ND means in summary, that you are free to “**Share**” (copy and redistribute the material in any medium or format), **but not modify** the aforementioned text for any purpose, even commercially, if you comply with the following obligation: **Attribution** - you must give [appropriate credit](https://creativecommons.org/licenses/by-nd/4.0/) and provide a link to the licence. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

**Liabilities**

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The authors who prepared this document bare no liabilities in relation to its use and implementation of the ideas, methods and advises contained therein.

**Clarification of Terminology**

The simultaneous use of male and female forms of speech has been avoided for reasons of better readability. All personal designations are equally applicable to both genders.

# Table of Contents

[A. Table of Contents 4](#_Toc497063996)

[B. Generic Information 6](#_Toc497063997)

[B1. Introduction 6](#_Toc497063998)

[B2. Organisation information within plan scope 6](#_Toc497063999)

[B3. Plan storage location 6](#_Toc497064000)

[B4. Plan objectives 6](#_Toc497064001)

[B5. Assumptions 7](#_Toc497064002)

[B6. Definitions 7](#_Toc497064003)

[B7. Roles, Responsibilities and Version control 8](#_Toc497064004)

[C. Incident and Crisis Management Plan 11](#_Toc497064005)

[D. Emergency Response and Evacuation Plan 15](#_Toc497064006)

[D1. Site covered 15](#_Toc497064007)

[D2. Emergency response plan goals and objectives: 15](#_Toc497064008)

[D3. Plan Preparation 15](#_Toc497064009)

[a) First Aid kit 15](#_Toc497064010)

[b) Lighting and warning system 15](#_Toc497064011)

[c) Fire extinguishers 15](#_Toc497064012)

[d) Designate an assembly point 16](#_Toc497064013)

[e) Evacuation Plan map and document 16](#_Toc497064014)

[D4. Response 17](#_Toc497064015)

[a) The (two) person(s) in charge of ordering an evacuation are 17](#_Toc497064016)

[b) Dealing with a fire 17](#_Toc497064017)

[c) When evacuating 17](#_Toc497064018)

[d) Upon arriving at the assembly area 18](#_Toc497064019)

[e) Next steps at the assembly area 18](#_Toc497064020)

[D5. Consider security of the premises 18](#_Toc497064021)

[D6. Other notes 18](#_Toc497064022)

[E. Insurance Plan 19](#_Toc497064023)

[F. Personnel Succession (Substitution) Plan 21](#_Toc497064024)

[G. Dealer, Third Party and Business Partner Failure Plan 22](#_Toc497064025)

[H. Donor/Sponsor Failure Plan 23](#_Toc497064026)

[I. IT Backup Plan 24](#_Toc497064027)

[J. Communication and Notification Plan 27](#_Toc497064028)

[J1. Persons responsible for communications 27](#_Toc497064029)

[J2. Organisation communication numbers and email addresses 27](#_Toc497064030)

[J3. Emergency notifications 29](#_Toc497064031)

[J4. Messages 29](#_Toc497064032)

[J5. Personnel and volunteer communication information 30](#_Toc497064033)

[J6. Stakeholders 31](#_Toc497064034)

[J7. Public Emergency Services and State authorities 31](#_Toc497064035)

[J8. Dealers, Third Parties and Business Partners 32](#_Toc497064036)

[a) Information on existing relations 32](#_Toc497064037)

[b) Information on potential alternatives 33](#_Toc497064038)

[J9. Key Donors/Sponsors 34](#_Toc497064039)

[K. Resources and Operations Recovery Plan 35](#_Toc497064040)

[K1. Roles and Responsibilities 35](#_Toc497064041)

[K2. Impact Table and Recovery Time Objectives 37](#_Toc497064042)

[K3. Activities Recovery prioritisation 39](#_Toc497064043)

[K4. Resource recovery plan 40](#_Toc497064044)

[a) Disaster recovery strategies in brief 40](#_Toc497064045)

[b) Resource recovery plan (failures and disaster incidents) 41](#_Toc497064046)

[K5. Typical disaster recovery response action list 49](#_Toc497064047)

[L. Information security incident response plan 52](#_Toc497064048)

[L1. Step 2: Detection – identification – understanding – evaluation 52](#_Toc497064049)

[L2. Step 3: Notification and escalation 53](#_Toc497064050)

[L3. Step 4: Response and crisis management 53](#_Toc497064051)

[M. Notes 54](#_Toc497064052)

# Generic Information

## B1. Introduction

This business continuity plan focuses on assisting the organisation to prepare itself to deal with threats and events that (may) cause disruptions to its operations and its ability to deliver services and products to its customers.

The plan documents the required information (actions, steps, data, etc.) that will assist the organisation's response team in dealing with any disruption and in resuming daily operations as normal to a predefined level and within a specific time interval.

## B2. Organisation information within plan scope

This plan covers organisation operations at the following site:

Floor / Room: <insert floor and room number if in building>

Address: <insert address> City: <insert city>

Phone: <insert > Fax: <insert > Email: <insert >

## B3. Plan storage location

This plan and its attachments are stored at the following off-site location(s), available for immediate access:

|  | Storage Location (\*) | Media (\*\*) |
| --- | --- | --- |
| Original document |  |  |
| Copy |  |  |

(\*) Provide address and detailed access information (it may be a directory on a server’s hard disk in an alternative office address). Make sure this information is sufficient to trace the document if and when required:

(\*\*) Paper copy, CD, web page in cloud etc.

## B4. Plan objectives

* To help the organisation to successfully respond to emergency events and life-threatening situations
* To help the organisation:
  + Manage facilities, assets and equipment failures
  + Deal with the failure of dealers or third parties
  + Handle personnel unavailability
  + Prepare alternative sources for vital records and resources
  + Manage insurance coverage
  + Manage a donor withdrawal
* To help the organisation:
  + Manage a disastrous incident and minimise its impact on the organisation
  + Restore organisation operations to a predefined level in a timely fashion
* To support the organisation’s resilience and ‘business as usual’ operational status

## B5. Assumptions

* This plan does not provide an approach for disastrous events at a regional or national level. However, it will greatly increase the organisation’s resilience and response capability.
* For a typical NGO, the number of personnel or volunteers available is usually limited, therefore a lack of employees might be a key issue for plan deployment. Alternatives have been predefined to assist in minimising this risk.
* Alternative sites (if any) are available and accessible.
* Critical information is stored off-site (data, backups, archives and vital records) and is accessible.
* This plan (as a document) is stored in an alternative site (or online in a cloud service) at its latest version and is immediately available when required.

## B6. Definitions

**Incident** is a situation that might constitute, or could lead to, disruption, loss, emergency or crisis.

**Disaster** is the result of an incident (equipment failure, severe weather conditions, natural disaster, vandalism, terrorist action etc.) related to:

* The loss (any or all) of
  + Facilities (site, assets, work area, systems)
  + IT Systems – Production systems
  + Connectivity (communications and systems access)
  + Utility service (power, water)
* The sudden unavailability of key personnel or volunteer
* The sudden failure of key dealers or business partners
* The disruption of organisation operations and / or the provision of any or all of its services
* Sudden withdrawal of a key donor/sponsor

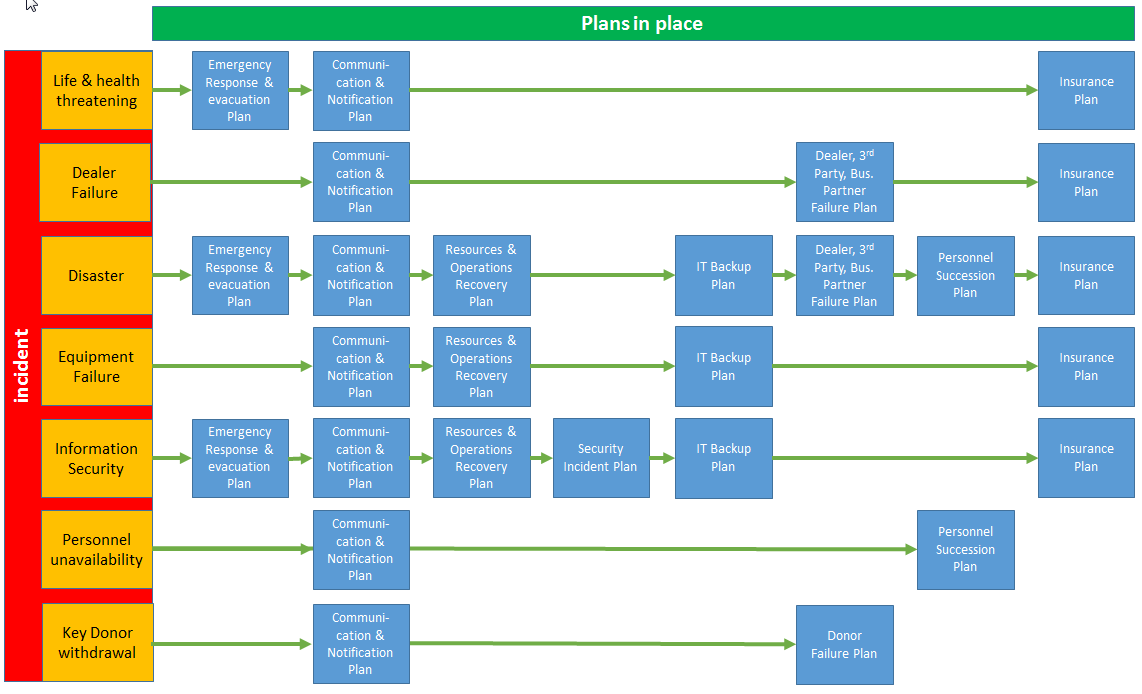
## B7. Roles, Responsibilities and Version control

The following table summarises key roles and responsibilities, from preparing the plan document(s) to managing plan deployment. Several or all plans may have the same owner.

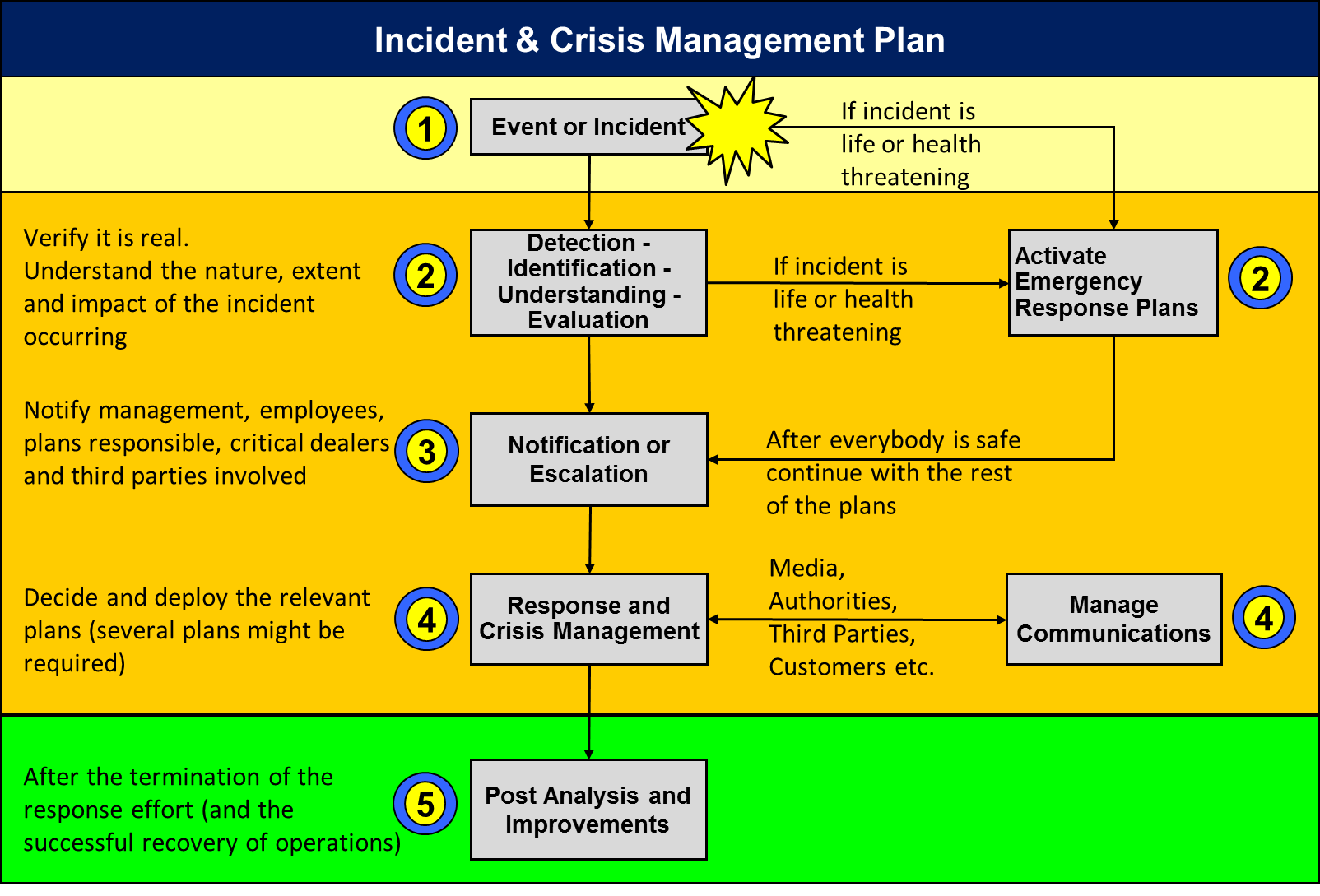
| Role | Responsibilities | Responsible person name | Deputy name | Date of last update | Date of next update |
| --- | --- | --- | --- | --- | --- |
| Incident Response Plan Manager | Manage the overall incident response effort |  |  |  |  |
| Emergency Response and Evacuation Plan Manager | Deploy the plan |  |  |  |  |
| Insurance Plan Manager | Deploy the plan |  |  |  |  |
| Employees Succession (substitution) Plan Manager | Deploy the plan |  |  |  |  |
| Dealer / Third Parties failure plan Manager | Deploy the plan |  |  |  |  |
| Donor / Sponsor Failure Plan Manager | Deploy the plan |  |  |  |  |
| IT Systems Backup Plan Manager | Deploy the plan |  |  |  |  |
| Communications Plan Manager | Deploy the plan |  |  |  |  |
| Failure and Disaster Recovery Plan Manager | Deploy the plan |  |  |  |  |
| Information Security Incident Response Plan Manager | Deploy the plan |  |  |  |  |
| BC Plan Document  Owner | Keep this document and all plans therein contained updated; ensure they are stored at the defined locations |  |  |  |  |

# Incident and Crisis Management Plan

The following is a diagram of all plans, whose use will depend on the nature of the incident. We must emphasise that this is an indicative approach and not all plans will be required in every situation (e.g. a false fire alarm may initiate the evacuation plan but may not require the insurance coverage plan). Details of each plan are in the relevant chapters.



When dealing with an incident, the following are typically the steps to follow:



**Step 1:** Incident occurs

* **If the incident is life or health threatening, deploy emergency response and evacuation plan IMMEDIATELY**

**Step 2:** Incident is detected by personnel or volunteers (by itself or due to some evidence of its occurrence or consequences)

* Ensure that the incident is real
* Try, based on objective evidence, to understand its nature (e.g. is it a fire, a security incident or a system failure?), the extent (e.g. loss of power to the whole neighbourhood vs loss of power failure to the office only) and the impact of the incident (e.g. the office area cannot be used due to severe damage e.g. from an earthquake)
* **If the incident is life or health threatening, deploy emergency response and evacuation plan IMMEDIATELY**

**Step 3:** Use the communication plan

* Notify organisation management, relevant personnel or volunteers and third parties / dealers who may help with the plan’s deployment and resolution (e.g. your IT dealer or consultant, your organisation’s legal advisor etc.)
* In certain cases (fire, theft etc.) it may be necessary to notify the relevant state authorities as well

**Step 4:** Manage the incident and (if required) the crisis

* Depending on the nature of the incident, its extent and the impacted areas, you may need to implement more than one plan (see picture in the previous chapter)
* If the impact of the incident and the uncertainties it creates (with regards to business continuity, organisational credibility or brand image) are high enough, you will need to manage the crisis. Using your common sense, work together with your personnel, volunteers, members, authorities, stakeholders and key partners (e.g. your legal advisor, your insurance agent etc.) to manage uncertainties, the negative impact and areas that are not under control in order to help operations get back to normal
* Always give thought to ongoing communication with key stakeholders (including the media) during the incident, and to crisis management

**Step 5:** Once the crisis is over and organisation operations have been resumed or returned to normal,

* Run a post-incident analysis of the root cause, and the organisation’s response performance to the incident
* Use the input to improve plans, minimise new risks identified and ensure that the organisation’s overall resilience is improved.
* Schedule the relevant meetings and discussions with your teams; identify improvements and implement these.
* Review the incident with your employees to raise their awareness of similar incidents in the future.

# Emergency Response and Evacuation Plan[[1]](#footnote-2)

## D1. Site covered

This plan is related to the <site name> site.

## D2. Emergency response plan goals and objectives:

* Evacuate personnel, volunteers and visitors from organisation site to the assembly area
* Notify related authorities and employees (building security, fire service, ambulance

service etc.)

* Provide first aid where required until the ambulance service arrives
* Notify organisation management and ensure the safety of personnel

## D3. Plan Preparation

### First Aid kit

* Prepare and have ready a first aid kit.
* Carry out an annual inspection and ensure that the last inspection date is clearly marked on the outside of the kit
* Make sure all personnel or volunteers are aware of where it is stored
* Every time you use something from the kit, ensure that it is replaced immediately

### Lighting and warning system

* Ensure that there is emergency lighting or easy-to-access flashlight in case of power outage
* Consider setting up a warning system (siren, alarm bell, etc.)
* Make sure your personnel and volunteers are aware of the specific sound(s) of the warning system and associate this with site evacuation

### Fire extinguishers

* Ensure fire extinguishers are in designated areas around the office with appropriate signage
* Ensure all personnel and volunteers know how to use them (run a simple instructional exercise for all employees)
* Check once annually that extinguishers have not passed their expiration date and that they are properly loaded

### Designate an assembly point

It is advisable to pick two alternative assembly points, one near your facilities and one in the nearby neighbourhood.

Both locations must be near your facility, safe for pedestrians and away from traffic lanes.

Assembly point 1: The address is: <insert assembly point 1 address here>

Assembly point 2: The address is: <insert assembly point 2 address here>

Insert a small map below

### Evacuation Plan map and document

* Prepare a floor and building evacuation map with emergency exits and escape route clearly marked
* Plan for two different exit routes out of the building (if this is possible)
* Evacuation map to be posted on the wall for quick reference by employees and visitors
* Keep a copy of this evacuation plan together with backup and/or continuity plans to provide to the fire service and other responders

## D4. Response

Every time an emergency or a threat to the health and safety of personnel, volunteers or visitors arises:

* Sound the alarm or notify by shouting
* Decide to evacuate (see person(s) responsible below)
* Evacuate
* Notify building security (if applicable)
* DIAL 112: If for fire, notify the fire service or other relevant services (at the same number), providing the office address
* Decide which assembly point to use (A or B)

### The (two) person(s) in charge of ordering an evacuation are

a) <insert name>

b) <insert deputy name>

### Dealing with a fire

If a fire breaks out in your office, remember two things:

* Your first priority is human lives, not property
* You are not a firefighter

Use the fire extinguishers only if the fire is very small or to help you evacuate safely.

Remember that a fire extinguisher contains only enough gas, water or foam to fight a fire for a matter of seconds, not minutes!

Run an exercise for all personnel and volunteers to familiarise them with the use of the fire extinguishers.

### When evacuating

* Close all doors behind you
* Cut off power
* Check to ensure no employees remain in the office
* Lock the outer office door, if this is safe to do
* Use the stairs. Walk fast, but do not overtake others
* Provide (if possible) a floor plan to the fire service or other responders

### Upon arriving at the assembly area

Make a list of all personnel and volunteers present at the assembly area

The highest-ranking staff member present may use the employee communication list (see communication plan) as a checklist to account for personnel and volunteers present.

If anyone is missing from the list of people in the office, communicate this immediately to the authorities on site (fire service, police).

### Next steps at the assembly area

Depending on the situation and once all personnel and volunteers are safely accounted for at the assembly point, you may decide to:

* Return to office, if it is safe to do so (if the authorities have granted permission)
* Initiate the disaster recovery plan or other contingency plans
* Ask all to return home (end of day)

In each case, consider the security of the assets, data and files in your office.

The senior leadership team of your organisation should be the persons responsible for taking this decision.

## D5. Consider security of the premises

Ensure the physical security of your premises. Depending on the situation, your approach may vary, e.g. if there is no access to the site (or building) or the building is seriously damaged, you may need to consider deploying external security to safeguard your assets and archives. You may consider communicating with neighbouring companies to coordinate a common approach.

Use common sense.

## D6. Other notes

<Add here any other notes related to your organisation emergency and evacuation plan>

# Insurance Plan

This is used to map the current insurance coverage of the organisation.

Insurance Agent Name:

Contact Information Address:

Phone: Fax: Email:

Current insurance coverage

| Insurance provider | Coverage area | Contract ID | Expiry date | What is covered | Cover amount | Limitations / Deductibles |
| --- | --- | --- | --- | --- | --- | --- |
| FIRM 1 | IT Systems loss / damage |  |  |  |  |  |
| FIRM 1 | Production systems loss / damage |  |  |  |  |  |
| FIRM 1 | Property / Site loss |  |  |  |  |  |
| FIRM 1 | Management Liabilities |  |  |  |  |  |
| FIRM 2 | Donations Loss |  |  |  |  |  |
| FIRM 2 | Organisation / Services Liability |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

<Add here any other notes related to your insurance plan>

Refer to (a) The time limitations for disaster notification established by your insurance provider (b) The records required by your insurance provider after an emergency.

Store the relevant documents in a safe place, together with your backups and other plans.

# Personnel Succession (Substitution) Plan

Fill in the table below. Bear in mind that if a person has several responsibilities, these may be covered by more than one person. In such a case, there may be more than one line per person.

| Employee / Member / Volunteer name | Position / responsibilities | Significance of position  (High, Medium, Low) | Name of potential successor (\*) | Readiness of successor to replace (full, partial, low) (\*\*) | Missing competencies (\*\*\*) | Action plan and schedule for successor to cover missing competencies |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

(\*) Name of the employee, volunteer or external partner who could replace (be a substitute for) the specific person

(\*\*) The percentage of the main personnel capabilities and capacity that the successor could cover

(\*\*\*) The competencies the Successor does not possess, meaning they are unable to fully cover this position

<Add here any other notes related to the personnel succession (substitution) plan>

# Dealer, Third Party and Business Partner Failure Plan

Fill in the table below. Use this plan to support your operations in case of the failure of any critical dealers, third parties or business partners.

| Dealer (partner / third party) | Products / services provided | Impact for the organisation of dealer failing | Maximum tolerable time of non-service by the dealer | Impact  (high, medium, low) | Alternative dealer / solution if dealer fails |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

<Add here any other notes related to dealer failure plan>

# Donor/Sponsor Failure Plan

Fill in the table below. Use this plan to support your operations in the case of any critical donor/sponsor withdrawing.

| Donor/Sponsor | % of support provided / overall donations | What is the impact on the organisation if donor withdraws | Maximum tolerable time of non-support by the donor | Criticality  (High, Medium, Low) | Alternative donor/solution if donor withdraws |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

<Add here any other notes related to donor failure plan>

# IT Backup Plan

Current backup strategy

| IT system /application | Function of the IT system | Importance of the IT system (\*) | What will be backed up (\*\*) | | | What files or directories are backed up (\*\*) | Frequency | Backup media used | Number of different copies | Backup storage area | Backup soft ware used | How to restore if main system lost | Restoration time estimated |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IT system files | Data  base files | Pro  grams |
| ERP Server | Hosts the organisation membership management application programme and data | High | YES | YES | YES | All | Every night, 23:00, Monday to Friday | External Hard disk | 5 copies. One different disk for every day | At ABC Bank Vault | FBKP soft ware is used | Download FBCK soft ware from web site, connect backup disk | 2-3 hours |
| Email | Communications with partners | Medium |  |  |  |  |  |  |  |  |  |  |  |
| Files in network drive | Donations list and donors details | High |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

(\*) High, Medium, Low

(\*\*) In several cases, not all data are backed up simultaneously. Other options might be available (e.g. incremental backup).

Describe in brief the typical process (including who runs the backup, when it is done, what is backed up, how it is done, how backups are transferred off-site, where copies are kept).

Special instructions:

* Backup is essential even if you automatically replicate the data from a primary location to another location, including use of cloud services. Data replication cannot save you from all risks (e.g. data corruption)
* Do not forget to back up files on PCs and laptops
* Ensure that all backups are encrypted. Ensure that you have safely stored the encryption key at a second address (e.g. manager’s home)
* If you use a bank vault, consider who will have authorised access to it
* Keep a daily log of each backup. Note the device ID (e.g. tape A or disk A). Check that the backup was completed successfully
* Ensure that you are able to restore your backups on alternative systems at an alternative location
* Replace defective media; destroy the old media

Test your backup

It is advisable to test your backups at specific time intervals (e.g. once every 3 months). Check that files and applications can be restored.

<Add here any other notes related to dealer failure plan>

# Communication and Notification Plan

## J1. Persons responsible for communications

a) <insert name>

b) <insert deputy name>

The above person(s) will be the point of contact for all personnel and volunteers during and after the event.

Ensure that all personnel and volunteers are aware of this.

## J2. Organisation communication numbers and email addresses

In case of an emergency, the following should be the organisation’s communication status:

| Type | Number / email Info | Provider | In case of disaster this line will be redirected to | Person responsible for redirection | Person responsible for responding during and after disaster | Notes |
| --- | --- | --- | --- | --- | --- | --- |
| Organisation call centre no. | +30 223344556677 |  |  |  |  |  |
| Organisation fax no. |  |  |  |  |  |  |
| Organisation email |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## J3. Emergency notifications

You may use the personnel, volunteers and members contact list below to notify them all during or after the emergency event. You may use the list to notify them about the initiation of the disaster recovery plan.

## J4. Messages

Define the organisation message for each stakeholder. This message may differ for each stakeholder, as their interests are different.

1. State authorities: provide all information necessary for them to handle the emergency effectively.
2. Personnel/Volunteers: provide information regarding the following:
   * What has occurred (information regarding the incident)?
   * Should they come to work?
   * When should they come to work?
   * How will this affect their jobs/work?
3. Organisation managers and stakeholders: provide full, detailed information regarding the incident
4. Donors/Sponsors: officers may be required to contact key donors, providing information primarily concerning the continuity of services offered and the expected recovery time
5. Beneficiaries: provide information about the incident and ensure the availability of products/services from your organisation and that they are available from them
6. Dealers, third parties and business partners: provide information regarding the incident and ask for specific assistance if required. Ensure also the availability of the products / services they provide to your organisation
7. The public / neighbours: depending on the incident, consider informing them of your efforts and the incident
8. The media: ensure that you have prepared a statements responding to questions regarding the organisation position on:
   * What happened?
   * Who was responsible?
   * How your organisation responded
   * Who, if anyone, was injured?

You may need (on a per case basis) to consult your legal advisor before providing a statement to the media.

## J5. Personnel and volunteer communication information

| Personnel/Volunteer name | Mobile phone no. | Home phone no. | Email (organisation / personal) | Home address | Notes |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## J6. Stakeholders

| Name | Mobile phone no. | Home phone no. | Email (organisation / personal) | Home address | Notes |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## J7. Public Emergency Services and State authorities

| Service / authority | Contact person  (if any) | Emergency phone no. | Standard phone no. | Notes |
| --- | --- | --- | --- | --- |
| Fire service |  |  |  |  |
| Police department |  |  |  |  |
| Emergency medical services |  |  |  |  |
| Electric power company |  |  |  |  |
| Water company |  |  |  |  |
| Civil protection authority |  |  |  |  |
| City emergency services |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## J8. Dealers, Third Parties and Business Partners

### Information on existing relations

| Company / Third Party | Service provided | Contact person | Direct / mobile phone | Standard business phone | Notes |
| --- | --- | --- | --- | --- | --- |
|  | Legal Advisor |  |  |  |  |
|  | Accountant |  |  |  |  |
|  | IT dealer |  |  |  |  |
|  | Communication (data / voice) provider |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### Information on potential alternatives

Fill in the table below with the communication information of alternative dealers and providers which may be used in the case of failure of current dealers or partners.

| Alternative company / Third party | Service provided | Contact person | Direct / mobile phone | Standard business phone | Notes |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## J9. Key Donors/Sponsors

Document your key donor/sponsor contact information

| Donor/Sponsor | Contact Person | Direct / mobile Phone | Standard Business Phone | Notes |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

<Add here any other notes related to Communications plan.>

# Resources and Operations Recovery Plan

## K1. Roles and Responsibilities

The following table summarises the key roles and responsibilities, from plan deployment to plan document management.

| Role | Title | Responsibilities | Name of responsible person | Name of deputy |
| --- | --- | --- | --- | --- |
| Disaster recovery plan team members | Decision maker | Person responsible for: initiating the plan (emergency, recovery etc.) |  |  |
| Head of crisis management and recovery effort | Person responsible for:  notifying team members, critical dealers |  |  |
| Team members | Person responsible for: notifying personnel, volunteers and stakeholders |  |  |
| Person responsible for: communicating with beneficiaries, the media |  |  |
| Person responsible for: participating in the recovery effort |  |  |
| Person responsible for: participating in the recovery effort |  |  |
| Person responsible for: recovering IT systems |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |  |
| Equipment failure response team | Responder | Failure of office equipment (fax, photocopiers etc.) |  |  |
| Failure of IT systems |  |  |
| Power and utilities failure |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## K2. Impact Table and Recovery Time Objectives

The following table will assist in defining the impact of a disruption to your organisation’s operations. Use the instructions in the guide to fill in the table.

| Impact | Length of disruption to operations  Indicate whether the impact of stopping operations is insignificant, minor, major or severe.  You may change the time intervals provided as examples below as per your organisation needs. | | | | | | | |  | Maximum tolerable period of disruption | Maximum recovery time |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0-12 h | 1  Day | 2 Days | 3  Days | 1 Week | 2 Weeks | 1 Month | Later |  |
| Loss of membership fees and donations |  |  |  |  |  |  |  |  | ➔ |  |  |
| Impact on cash flow |  |  |  |  |  |  |  |  | ➔ |  |  |
| Increase in expenses |  |  |  |  |  |  |  |  | ➔ |  |  |
| Regulatory and other legal impacts |  |  |  |  |  |  |  |  | ➔ |  |  |
| Contract penalties |  |  |  |  |  |  |  |  | ➔ |  |  |
| Beneficiaries dissatisfaction |  |  |  |  |  |  |  |  | ➔ |  |  |
| Loss of donors |  |  |  |  |  |  |  |  | ➔ |  |  |
| Negative brand image and reputation |  |  |  |  |  |  |  |  | ➔ |  |  |
| At organisation level | | | | | | | | | 🡻 |  |  |

**ORGANISATION-LEVEL RECOVERY TIME OBJECTIVE:**

## K3. Activities Recovery prioritisation

The following table will assist in prioritising organisation activities during recovery. Use the instructions in the guide to fill in the table.

| Main processes / activities | Critical dates, periods related to the activity | Internal dependencies,  systems, applications, other processes | External dependencies (Dealers, Third parties etc.) | Maximum tolerable period of disruption | Recovery time objective |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## K4. Resource recovery plan

### Disaster recovery strategies in brief

Outline in brief an alternative strategy for the following:

**Targeted recovery time** (indicate the number of hours or days until organisation operations resume)

**Alternative working area** (designate an alternative working area for **personnel and volunteers**. Provide full address and area map)

**Alternative IT systems and communications** (outline the approach regarding IT systems if those at the main site are lost. Include a consideration of data recovery)

**Alternative office and production equipment** (outline the approach regarding office systems – computers, fax machines etc., and any production equipment, if those at the main site are lost)

### Resource recovery plan (failures and disaster incidents)

The following tables cover organisation resources of all kinds, in relation to both failures and disaster incidents. You may add in missing information.

The data provided are examples only.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Personnel and Volunteers (numbers during normal operations and at alternative work areas and relocations) | | | | |
| Details or personnel name | Normal operations status and quantities | Alternative site strategy (where they will work from) | Expected recovery time | Describe how they will have access to applications, files, email etc. |
| Manager | 1 | Work from home with personal laptop | Start from day 1 | Will use internet to access the cloud applications |
| Officers | 2 | Work from home for 2 weeks. Will have to buy 2 laptops on day 1 | Start from day 2 |  |
| Secretary | 1 | Will use the office at the XYZ collocation centre, where the company has rented an area |  |  |
| Accountant | 1 |  |  |  |
| Volunteers |  |  |  |  |

| Information Technology – Systems, Soft Ware and Applications – Office Equipment – Communication lines | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Resources | | Malfunction or failure | | Disaster solution (complete loss of existing) | | |
| Details | Normal operations status and quantities | Current approach / solutions in place / support contract / alternatives in place | Expected repair / replacement time | Alternative solution description | Expected recovery Time | Expected quantity available |
| Applications and Soft Ware | | | | | | |
| ERP Membership Management Application | Access for 3 people | Ad hoc support by ERP- dealer (there is a support contract in place) | Response within 2 hours as of contract | ERP is also replicated to a cloud version. After disaster, we will work with cloud (after data restore) | Day 2, Day 1 will be used by ERP-Dealer to restore data | Access for 3 people |
| Email application | 5 people |  |  |  |  |  |
| MS-Office soft ware | 5 people |  |  |  |  |  |
| File Server | Server, 3 TB disk |  |  |  |  |  |
| Mail and File | Server,  2 TB disk |  |  | New server will be bought. Restore files from backup. Will be installed at the alternative relocation site | 3rd day, including purchase, set-up and restore |  |
| IT Systems and devices | | | | | | |
| Laptops | 3 | There is always 1 PC/Laptop extra in the office until the failed is repaired | 1-3 days | Will buy 3 laptops from electronics store | Requires 2 days, including purchasing and set-up | 3 pieces |
| Desktop PCs | 3 |  |  |  |  |  |
| Laser Printer | 1 |  |  |  |  |  |
| Inkjet Printer | 1 |  |  |  |  |  |
| Firewall | 1 |  |  |  |  |  |
| Siemens Telephone Centre | 4 in 4 out lines,  5 devices |  |  | Redirect lines to a mobile.  Personnel will use their mobile phones | Day 2 |  |
| Fax Device | 1 |  |  |  |  |  |
| Photocopier | 1 | Repair as per existing contract | Response within 2 hours as of contract | Will use the printer-scanner device at the alternative site | Day 2 | 1 |
|  |  |  |  |  |  |  |
| Office equipment | | | | | | |
| Desks | 5 |  |  |  |  |  |
| Chairs | 7 |  |  |  |  |  |
| Closets | 4 |  |  |  |  |  |
| Vault | 1 |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Production equipment | | | | | | |
| Book Printing machine | 1 | Repair as per existing contract |  | Will outsource printing to Dealer A | Day 3 |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Communication lines (Data and voice) | | | | | | |
| 5599887766 | 4 i-o voice lines | Call telecom provider | In a few hours | Redirect to mobile (see communication plan) | 1-2 hours | 1 |
| Internet line |  | Call telecom provider | In a few hours | Use mobile internet to temporarily tether |  |  |
| 4488996655 | 1 fax line |  |  |  |  |  |
|  |  |  |  |  |  |  |

| Files and Archives (all kinds) | | | | |
| --- | --- | --- | --- | --- |
| Description of archive | Current Storage Location | Media Type | Alternative Source if archive is lost.  How it will recover to be available | Expected Recovery Time |
| Original Donations Agreements | Accounting closets | Paper,  electronically scanned | Re-print from scanned copies (stored in the organisation file server). Will recover once the file server is recovered | Day 3 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## K5. Typical disaster recovery response action list

The following is a typical action list for responding to a disaster incident. Bear in mind that a disaster incident may occur during business hours or outside of them; therefore, you may need to enrich the information supporting both scenarios (day and night), based on your individual needs.

| **No** | **Task / activity** | **Person responsible / notes** | **Done** |
| --- | --- | --- | --- |
| **1** | Ensure personnel and volunteer safety  Activate emergency response and evacuation plan if required |  |  |
| **2** | Make a note of the incident time and the notification time |  |  |
| **3** | Review incident information and assess the extent of damages. Evaluate impact to operations |  |  |
| **4** | Consider communicating with:   * Building security * Authorities and local government agencies * Neighbours * Etc.   depending on the event |  |  |
| **5** | Decide on whether to initiate BC plan |  |  |
| **6** | Notify recovery team and personnel |  |  |
| **7** | Retrieve BC plan document (from storage area)  Retrieve backup media (from storage area)  Review priorities and objectives with team  Review available resources  Estimate recovery time for services and operations |  |  |
| **8** | Manage communication with (on a need to know basis):   * Personnel and volunteers and/or families * PR and the media * Stakeholders * Key dealers (including IT systems and applications) * Beneficiaries |  |  |
| **9** | Contact alternative facilities to notify regarding disaster recovery use of the facility (if applicable) |  |  |
| **10** | Contact insurance company and key dealers |  |  |
| **11** | Relocate to alternative facility (or implement the arrangements you have planned) |  |  |
| **12** | Recover systems, applications, communications and other resources, as planned.  Arrange for purchase of missing equipment etc.  Check cashflow |  |  |
| **13** | Contact local government agencies  (tax office, regulatory authorities etc.)  Contact bank(s) |  |  |
| **14** | Communicate information to key donors  (if applicable) |  |  |
| **15** | Once recovery has been accomplished, review status and determine long-term strategy |  |  |
| **16** | Project manage restoration of the damaged site or relocation to a new one, depending on the extent and nature of the damage |  |  |
| **17** | Review this plan and prepare enhancements and improvements, based on lessons learned from the incident |  |  |

# Information security incident response plan

The information security incident response follows similar steps to the typical incident management plan.

The five steps of incident management are the same, with the following additions and considerations:

## L1. Step 2: Detection – identification – understanding – evaluation

**Detecting a security incident can be:**

* Straightforward i.e.:
  + Complete failure of an IT system
  + A missing system, device or file
  + …
* Suspected by identifying and understanding specific signs as:
  + System alerts appearing on users’ screens
  + Antivirus software alerts regarding an infected system
  + Inability to access a system or an application or browse the internet
  + Arrival of a large number of emails with suspicious content
  + A rapid deterioration in network traffic
  + Filenames with unusual characters
  + An unfamiliar username within the organisation’s system
  + Missing data
  + Data seemingly altered without any reason or without the knowledge of the system administrator(s)
  + A change to the appearance and/or content of the organisation’s web page or intranet pages (menus or content).
  + …

**Try to identify:**

* Which systems have been affected?
* Is the incident over, or might the intrusion still be occurring?
* Has confidential information been leaked? If so, to what extent?
* Are there any possible legal or regulatory consequences due to the potential incident?

Detecting and identifying security breaches and incidents is usually difficult for the average NGO employee who is unlikely to be an IT expert. Taking the above into account, proceed to Step 3.

## L2. Step 3: Notification and escalation

Consider the following:

* Notify the appropriate people within the organisation. **Communicate with and involve the organisation’s IT dealer or consultant.**
* Depending on the incident, it may be necessary to notify other or all system dealers and/or other external organisations, asking for assistance in dealing with the incident.
* Use discretion when discussing details of an incident with others; notify only those who need to know.
* Use secure communication channels: if your email services have been attacked, then do not use email.

## L3. Step 4: Response and crisis management

Consider the following:

* Determine together with organisation management and your IT Consultant whether you should proceed to any of the following steps:
* Disconnecting affected systems from the network
* Stopping network traffic
* Notifying third parties that may have been or may be harmed (e.g. notifying beneficiaries whose IT systems are connected to your systems)
* Notifying and working with your legal advisor
* Notifying and working with the police and your IT consultant to locate the intruder(s) and take legal action against them

If the incident is related to hacking or a related malicious act, legal prosecution will require specific evidence. Take care not to destroy evidence or information. Collect, document and preserve the information:

* Incident description
* List of affected systems
* System logs
* Backups of affected systems
* Response actions performed

Follow your IT dealer or consultant’s advice regarding the recovery approach and process. Recovery may require:

* Wiping out all vulnerabilities (removing malware, viruses etc.)
* Restoring missing or damaged data
* Implementing your disaster recovery solutions until main systems are back online.

# Notes

Insert here any other notes, diagrams, IT instructions, etc. that may assist you in the recovery effort.





1. Usually this Plan is obligatory to be in place for every organisation in all countries. [↑](#footnote-ref-2)