holibob

Crisis and Incident Management Policy

Version: 2

15 April 2024

Table of Contents

1 Policy 1
2 Strategy 1
3 Business Continuity 2
4 Introduction 2
4.1 Responsibilities 3
4.2 Initial safety actions for staff 4
4.3 Business process principles 4
4.4 Business Resumption 5
4.5 IT Recovery 5
4.6 Contact with our Partners 6
4.7 Communication 6
4.7.1 Media Contact 6
4.8 Testing and Exercises 6

1 Policy

A Crisis and Incident Management Policy typically includes the following components:

1. Purpose: A statement of the policy's purpose, which is to establish a framework for managing crises and incidents within the organization.
2. Scope: A description of the types of crises and incidents covered by the policy, including cybersecurity incidents, natural disasters, and other emergencies.
3. Roles and Responsibilities: A description of the roles and responsibilities of individuals and teams within the organization for managing crises and incidents, including crisis management teams, incident response teams, and business continuity teams.
4. Incident Response Plan: Develop an incident response plan that outlines the steps to be taken in the event of a crisis or incident, including notification procedures, escalation procedures, and communication protocols.
5. Crisis Management Plan: Develop a crisis management plan that outlines the steps to be taken in the event of a major crisis, including procedures for activating the crisis management team, establishing a command center, and coordinating response efforts.
6. Business Continuity Plan: Develop a business continuity plan that outlines the steps to be taken to ensure that critical business functions can continue in the event of a crisis or incident, including procedures for restoring systems and data, and for communicating with stakeholders.
7. Testing and Training: Regularly test and train employees on the incident response, crisis management, and business continuity plans to ensure that they are effective and up-to-date.
8. Communication: Develop a communication plan that outlines the procedures for communicating with internal and external stakeholders during a crisis or incident, including employees, customers, partners

2 Strategy

A Crisis and Incident Management strategy typically involves the following steps:

1. Risk Assessment: Conduct a comprehensive risk assessment to identify potential crises and incidents that could impact the organization, including natural disasters, cybersecurity incidents, and other emergencies.
2. Incident Response Plan: Develop an incident response plan that outlines the steps to be taken in the event of a crisis or incident, including notification procedures, escalation procedures, and communication protocols.
3. Crisis Management Plan: Develop a crisis management plan that outlines the steps to be taken in the event of a major crisis, including procedures for activating the crisis management team, establishing a command center, and coordinating response efforts.

4. Business Continuity Plan: Develop a business continuity plan that outlines the steps to be taken to ensure that critical business functions can continue in the event of a crisis or incident, including procedures for restoring systems and data, and for communicating with stakeholders.
5. Training and Testing: Regularly train employees on the incident response, crisis management, and business continuity plans, and conduct regular testing exercises to ensure that they are effective and up-to-date.
6. Communication: Develop a communication plan that outlines the procedures for communicating with internal and external stakeholders during a crisis or incident, including employees, customers, partners, and regulatory authorities.
7. Recovery: Develop and implement recovery procedures to restore critical business functions and systems in the event of a crisis or incident, and ensure that employees are trained on these procedures.
8. Evaluation and Improvement: Regularly evaluate the effectiveness of the crisis and incident management strategy, and make improvements as necessary to ensure that it remains effective and up-to-date.

Overall, a Crisis and Incident Management strategy should be designed to ensure that the organization is prepared to respond quickly and effectively to potential crises and incidents, and to minimize their impact on the business. By implementing a comprehensive set of measures, including risk assessment, incident response,

3 Business Continuity

4 Introduction

Physical locations, assets, data and staff are critical to the operation of an organisation and the service it provides to its service users. Therefore, there's a need to be able to restore service operations, following a 'disaster', as soon as it's possible.

The purpose of a plan is to maximise the ability of the organisation to recover from such a disaster, if one occurs. For this purpose, a disaster would be anything threatening the continuity of the organisation's core business. This includes:

- a fire
- a bomb (terrorism)
- an explosion (gas)
- a pandemic
- severe weather conditions

In a disaster situation there's an initial sense of shock, followed by a team spirit with everybody wishing to help. The team spirit will exist not only from the staff, but also from the general public.

This team spirit of co-operation will last for a few days, but a lack of interest will set in if people see that they're not being given any direction or assistance. For example, the inability to carry out services (supervising users through group work, one to one support, payment of staff) will lead to stress and complaints.

Getting the 'essentials' back up and running speedily should be the priority.

Responsibility for this program has been given to <Organisation> management. Your co-operation with these efforts will help us to maintain a program that accomplishes its goals.

4.1 Responsibilities

It's the responsibility of the <role>, to ensure that disaster recovery plans are in place and available for all sites. These plans are to be checked, distributed and tested on a regular basis, but at least annually.

Copies of this plan, and up to date site information sheets, are located <location>. 'Controlled' copies are reissued by:

<role>

<role>

<role>

all caseworkers

<role>

all administrators

<role>

Depending on the site and nature of the disaster, various members of staff from different functions will form the 'Disaster Recovery Team', who'll each be assigned specific tasks.

In the event of a major terrorist activity, the whereabouts of staff potentially visiting or travelling through the affected area on business, should be reviewed.

4.2 Initial safety actions for staff

- Ensure that all staff and visitors have been evacuated from the building to a safe area.
- Liaise with the emergency services (if in attendance).
- Identify the number of potential casualties.
- Ensure no staff or members of the general public enter any area classed as unsafe.

Contact with the following emergency services should be made.

1. <Role>, <Name> - <Contact Number>.

4.3 Business process principles

Team seniors should draw up a list of priorities for work with staff, assessing what can be achieved when and by who.

Following consultation with the <role> this should be communicated to:

- Our Partners

Where data information has been temporarily lost as a result of a disaster, encrypted backups held offsite should be used to restore information lost on the previous business day.

Where necessary, a contracted IT company should be able to assist with restoring data onto servers over time. Client information through online systems should be available.

In the event of complete internet failure, an additional wireless router with local area network (LAN) connectivity should be obtained and plugged into the main router for internet access.

A hard copy backup of contacts and client contacts should be kept and updated monthly by staff.

4.4 Business Resumption

This details the process that determines when and how the organisation returns to 'normal' operation. This would change depending on the nature of the disaster, so it's difficult to outline.

Generally, the management team will draw up a solution and develop an implementation plan. It's important to stress that it may take considerable time to rebuild or relocate to a new building.

4.5 IT Recovery

The responsibility of IT recovery lies solely with the IT Provider.

Major incidents are to be reported to them through the Office Manager. Telephony services will be the responsibility of the Office Manager.

4.6 Contact with our Partners

Contact arrangements may need to be re-established and co-ordinated by the individual caseworkers for each project.

Signs or notices on disaster sites can direct users to a new location or give temporary contact details, identifying 'business as usual' details.

Use of announcements on social media and in the local press or on local radio stations may assist in increasing the awareness of temporary arrangements.

4.7 Communication

Incorrect statements may be made to the press and general public, and rumours may start. This will give the impression of a general state of disorganisation and will reflect badly on the service for years to come. Therefore, all communications, and delivery of such messages, will be the responsibility of the <role> or the <role>.

4.7.1 Media Contact

This will be handled by the <role> or the <role>.

- What has happened
- What we're doing about it
- What actions are being implemented to provide services to the public
- Regular updates on the situation and how it may affect them

4.8 Testing and Exercises

We will conduct testing and exercises annually to evaluate the effectiveness of our preparedness program, make sure employees know what to do and find any missing parts.

There are many benefits to testing and exercises.

These include to:

- train personnel – clarify roles and responsibilities
- reinforce knowledge of procedures, facilities, systems and equipment
- improve individual performance – as well as organizational co-ordination and communications
- evaluate policies, plans, procedures and the knowledge and skills of team members
- reveal weaknesses and resource gaps
- comply with local laws, codes and regulations
- gain recognition for the emergency management and business continuity program