**Disclaimer:**

This Organisation Continuity Plan template is provided for general informational purposes only. It is not a substitute for professional advice, and users should adapt it to their specific needs and circumstances. While this template is based on best practices, L2 Cyber Security Solutions make no warranties or guarantees regarding its effectiveness or suitability for any particular situation. Users are responsible for ensuring the accuracy and completeness of the plan for their organisation. This template does not constitute legal advice, and users should consult with legal counsel for their specific legal needs. Organisation resilience best practices evolve, and users are encouraged to stay updated on industry standards. It is crucial to regularly test and revise this plan to ensure its effectiveness.

**[Your Organisation Logo]**

**[Organisation Name]**

Organisation Continuity Plan (OCP)

Version: 1.0

Date: **[Date]**

Contents

[1. Executive Summary 4](#_Toc160443225)

[1.1 Purpose 4](#_Toc160443226)

[1.2 Scope 4](#_Toc160443227)

[1.3 Key Contacts 4](#_Toc160443228)

[1.4 Plan Objectives 4](#_Toc160443229)

[2. Introduction 4](#_Toc160443230)

[2.1 Background 4](#_Toc160443231)

[2.2 Document Overview 4](#_Toc160443232)

[3. Organisation Impact Analysis (OIA) Summary 4](#_Toc160443233)

[3.1 Critical Organisation Processes 4](#_Toc160443234)

[3.2 Recovery Objectives 4](#_Toc160443235)

[3.3 Risk Assessment 5](#_Toc160443236)

[4. Risk Management 5](#_Toc160443237)

[4.1 Risk Identification and Assessment 5](#_Toc160443238)

[4.2 Risk Mitigation Strategies 5](#_Toc160443239)

[5. Organisation Continuity Strategies 5](#_Toc160443240)

[5.1 Recovery Team Roles and Responsibilities 5](#_Toc160443241)

[5.2 Incident Response and Escalation 6](#_Toc160443242)

[5.3 Communication Plan 6](#_Toc160443243)

[5.4 Alternate Worksite Procedures 6](#_Toc160443244)

[6. Plan Activation and Execution 6](#_Toc160443245)

[6.1 Activation Triggers 6](#_Toc160443246)

[6.2 Incident Command 6](#_Toc160443247)

[6.3 Recovery Procedures 6](#_Toc160443248)

[6.4 Resource Allocation 6](#_Toc160443249)

[6.5 External Support and Coordination 6](#_Toc160443250)

[7. Testing and Maintenance 6](#_Toc160443251)

[7.1 Testing Schedule 6](#_Toc160443252)

[7.2 Test Scenarios 6](#_Toc160443253)

[7.3 Test Results and Improvements 6](#_Toc160443254)

[7.4 Plan Maintenance 6](#_Toc160443255)

[8. Training and Awareness 6](#_Toc160443256)

[8.1 Employee Training 6](#_Toc160443257)

[8.2 Awareness Programs 7](#_Toc160443258)

[9. Plan Review and Update 7](#_Toc160443259)

[9.1 Regular Review Schedule 7](#_Toc160443260)

[9.2 Post-Incident Review 7](#_Toc160443261)

[10. Appendices 7](#_Toc160443262)

[10.1 Building/Site Information 7](#_Toc160443263)

[10.2 Staff Contact List 7](#_Toc160443264)

[10.3 Service User Contact List 7](#_Toc160443265)

[10.4 Other Office Contact List 8](#_Toc160443266)

[10.5 External Vendors/Partners Contact List 8](#_Toc160443267)

[10.6 Office Furniture, Fixtures, Fittings and Equipment 8](#_Toc160443268)

[10.7 Document Revision History 8](#_Toc160443269)

[10.8 Glossary of Terms 8](#_Toc160443270)

# 1. Executive Summary

## 1.1 Purpose

The Organisation Continuity Plan (OCP) aims to ensure the resilience of the organisation in the face of disruptions by defining strategies, procedures, and responsibilities for effective response and recovery.

## 1.2 Scope

This plan covers critical operational processes, risk management, recovery strategies, testing, and training.

## 1.3 Key Contacts

List key personnel and their contact information.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Mobile Number** | **Alternative contact** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 1.4 Plan Objectives

Outline the objectives of the OCP, including:

Ensuring the safety of employees and stakeholders.

Minimising financial losses during disruptions.

Maintaining essential operations.

Safeguarding the organisation's reputation.

# 2. Introduction

## 2.1 Background

Provide a brief background explaining the need for an OCP, including recent incidents or events that highlight its importance.

## 2.2 Document Overview

Explain the structure and purpose of this document, guiding readers through its sections.

# 3. Organisation Impact Analysis (OIA) Summary

## 3.1 Critical Organisation Processes

List and describe the critical operational processes that are vital for the organisation's operations – from section 6 of the OIA.

## 3.2 Recovery Objectives

Specify the recovery objectives for each critical operational process, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) – from section 4 of the OIA.

## 3.3 Risk Assessment

Summarise the results of the risk assessment, highlighting potential threats and vulnerabilities identified – from section 5 of the OIA.

# 4. Risk Management

## 4.1 Risk Identification and Assessment

Detail the process of identifying risks and vulnerabilities within the organisation, including the sources of threats and explain how risks are assessed, categorised, and prioritised based on their potential impact and likelihood. – from section 5 of the OIA.

## 4.2 Risk Mitigation Strategies

Describe the strategies and measures in place to mitigate identified risks.

# 5. Organisation Continuity Strategies

## 5.1 Recovery Team Roles and Responsibilities

Define the roles and responsibilities of the OCP recovery team members.

* The OCP Team has overall responsibility for operational continuity for the organisation. It is made up of the OCP Team Leader, and the Team Leaders of the other teams in the structure. An OCP Deputy Team Leader should also be considered, in case the Team Leader is absent.
* The OPR Team is responsible for the recovery of the individual operational processes that are carried out within the organisation. The team would be made up of the people who are responsible for the recovery of each process.
* The IT Recovery Team is responsible for the recovery of any and all affected systems and applications. This team is made up of the staff responsible for the recovery of the organisation’s IT Infrastructure.
* The Recovery Support Team is responsible for ancillary support to the recovery process. This would include HR, Payroll, ongoing Communications with service users, etc. If there is a large HR or other accounting function within the office, it may need an OPR team of its own.

## 5.2 Incident Response and Escalation

Outline the steps to be taken during the incident response phase, including escalation procedures.

## 5.3 Communication Plan

Detail the communication strategies for informing employees, stakeholders, and the public during disruptions.

## 5.4 Alternate Worksite Procedures

Describe procedures for relocating operations to alternate worksites if necessary.

# 6. Plan Activation and Execution

## 6.1 Activation Triggers

Identify the conditions or events that trigger the activation of the OCP.

## 6.2 Incident Command

Explain how the incident command structure will operate during a crisis.

## 6.3 Recovery Procedures

Provide step-by-step procedures for executing the OCP during disruptions.

## 6.4 Resource Allocation

Describe the allocation of resources, including personnel, equipment, and financial resources.

## 6.5 External Support and Coordination

Detail how the organisation will coordinate with external agencies, partners, or vendors for support.

# 7. Testing and Maintenance

## 7.1 Testing Schedule

Outline the schedule for regular OCP testing and exercises.

## 7.2 Test Scenarios

Describe various test scenarios that will be used to evaluate the effectiveness of the plan.

## 7.3 Test Results and Improvements

Explain how test results will be documented and used to improve the OCP.

## 7.4 Plan Maintenance

Specify the process for updating and maintaining the OCP to reflect changes in the organisation's operations or environment.

# 8. Training and Awareness

## 8.1 Employee Training

Explain the training programs in place to ensure that employees understand their roles in the OCP.

## 8.2 Awareness Programs

Detail awareness initiatives aimed at promoting a culture of preparedness.

# 9. Plan Review and Update

## 9.1 Regular Review Schedule

Outline the schedule for reviewing and updating the OCP to ensure its relevance.

## 9.2 Post-Incident Review

Explain the process for conducting post-incident reviews to identify lessons learned and areas for improvement.

# 10. Appendices

## 10.1 Building/Site Information

|  |  |
| --- | --- |
| **Building/Facility Manager** | **Details** |
| Name |  |
| Address |  |
| Main Telephone Number |  |
| 24 Hour Telephone Number |  |
| E-mail Address |  |

|  |  |  |
| --- | --- | --- |
| **Other Numbers/Utilities** | **Name** | **Contact Number(s)** |
| Local Gardai/Police |  |  |
| Local Authority (Council) |  |  |
| Electricity Provider |  |  |
| Water Provider |  |  |
| Building Security |  |  |
| Alarm Monitoring Station |  |  |
| Building Insurer |  |  |
| Telephony Provider |  |  |
| Data Communications Provider |  |  |

## 10.2 Staff Contact List

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Address** | **Phone** | **Personal Email** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 10.3 Service User Contact List

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Address** | **Main Contact** | **Phone** | **Email** | **Who makes contact** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 10.4 Other Office Contact List

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Address** | **Main Contact** | **Phone** | **Email** | **Who makes contact** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

This list should include all Internal contacts at other premises that are part of your organisation unit and that may be dependent on your office, or to whom your office is dependent, including internal IT personnel.

## 10.5 External Vendors/Partners Contact List

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Service Provided** | **Name** | **Address** | **Main Contact** | **Phone** | **Email** | **Who makes contact** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

This list should include all vendors, suppliers and partners on whom your organisation is dependent. This should include Banks, Regulators, Off-site Storage, Office Supplies, Stationers, Office Equipment Providers, IT Equipment providers, IT service vendors, Telephony suppliers, etc.

## 10.6 Office Furniture, Fixtures, Fittings and Equipment

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Make and Model** | **Quantity** | **Supplier** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

This list would **exclude** any IT equipment, as this should be included in the IT Disaster Recovery Plan.

## 10.7 Document Revision History

Maintain a record of document revisions, including dates and descriptions of changes.

## 10.8 Glossary of Terms

Define any specialised terms or acronyms used in the document.

This template provides a structured framework for creating a comprehensive Organisation Continuity Plan (OCP) tailored to your organisation's needs. Customise the content within each section to match your specific requirements and circumstances.