

Disaster Recovery Plan

Classification: **Internal**

This document may not be shared externally without written approval from the document owner.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|  |  |  |  |  |  |  |

Contents

[Purpose of Document 2](#_Toc168852413)

[Policy 2](#_Toc168852414)

[Scope 2](#_Toc168852415)

[Summary of Architecture & Services 2](#_Toc168852416)

[Invocation Process 3](#_Toc168852417)

[Risk Assessments 5](#_Toc168852418)

[Disaster 7](#_Toc168852419)

[Key External Contacts 7](#_Toc168852420)

[Hierarchy of Notifications 8](#_Toc168852421)

[Comms Plan 9](#_Toc168852422)

[Contact list - Key Stakeholders 9](#_Toc168852423)

[Testing 10](#_Toc168852424)

[Document Maintenance 10](#_Toc168852425)

[Key Reference Materials 11](#_Toc168852426)

[Vendor SLA Agreements 11](#_Toc168852427)

[Important Information 11](#_Toc168852428)

[Backup Summaries 12](#_Toc168852429)

[Recovery Procedures 12](#_Toc168852430)

Purpose of Document

The following disaster recovery plan (DRP) is designed to assist [Company Name] in preparing for and recovering from disruptive events, such as the loss of a site, service, cyber-attacks, power outages, or other incidents that could result in data loss or system downtime.

The key reasons for the DRP are as follows.

* **Minimising Downtime**: By having a DRP in place, [COMPANY NAME] can reduce the time that its IT systems are offline and minimise the impact of a disaster on its operations and, therefore, impact upon its customers.
* **Protecting data**: A DRP helps ensure that critical data is backed up regularly and can be restored quickly in a disaster, reducing the risk of data loss.
* **Enhancing business resilience**: A DRP helps [COMPANY NAME] become more resilient and better prepared to deal with unexpected events or disruptions.
* **Maintaining customer confidence**: With a DRP in place, [COMPANY NAME] can demonstrate to customers and stakeholders that it takes business continuity seriously and is committed to maintaining operations in the face of unexpected disruptions.

Policy

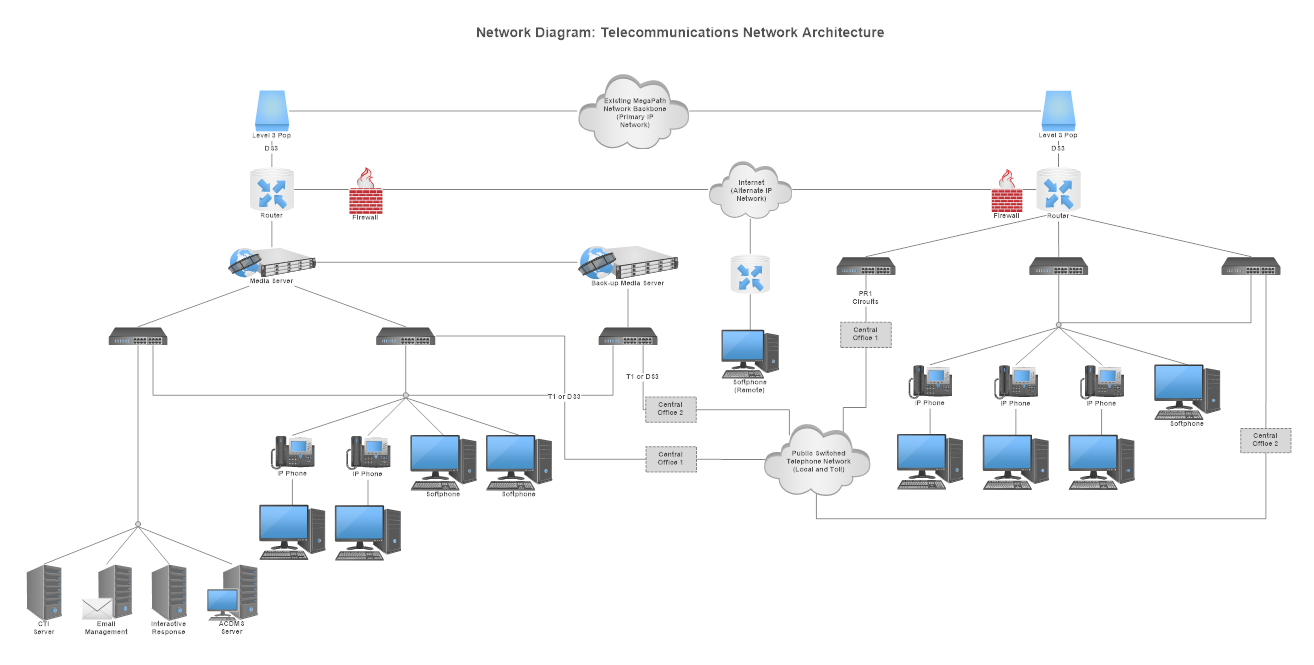
* The Head of Engineering is accountable for ensuring this document is reviewed and tested annually.
* The DRP shall cover all critical IT infrastructure, including systems and networks.
* All staff responsible for executing and maintaining the DRP will be trained appropriately.
* Procedures for recovery will be kept up to date as soon as any changes are made.

Scope

## Summary of Architecture & Services

The scope of this DRP is for the recovery of [COMPANY NAME] product services. It is not a Business Continuity plan and does not address broader issues of building infrastructure, employee management, customer communications and business processes.

The infrastructure of [Company Name] comprises a multi-tiered architecture designed to support a scalable tenant-landlord ecosystem.



Key services include client-facing applications, internal administration interfaces, development operations, and analytics.

Core functionalities are facilitated through a combination of cloud-hosted services, including [Insert summary of SaaS technologies used]

The architecture supports continuous integration and deployment (CI/CD), with [If you have a development pipeline, summarise the tools here].  
  
The system's resilience is critical for maintaining uptime and ensuring data integrity for all stakeholders involved in the moving process.

# Invocation Process

The following steps outline the process to declare a disaster and activate the disaster recovery plan formally:

|  |  |
| --- | --- |
|  | The incident lead (typically the Head of Engineering) will assess the incident to determine if it meets the criteria for a disaster declaration. |
|  | The incident lead will confer with the DR team members to review the assessment and gain consensus on formally declaring a disaster. |
|  | If the event meets the disaster declaration criteria, the incident lead will formally activate the DR plan and turn incident management over to the DR team. |
|  | The incident lead will notify senior management of the disaster declaration and DR activation. |
|  | The DR team will follow the procedures and checklists outlined in the DR plan to recover critical systems and functions. |
|  | External partners and vendors will be engaged as needed to provide additional resources and capabilities. |
|  | The DR team will execute the communications plan to inform impacted stakeholders of progress. |
|  | Once critical systems have been recovered, the DR team will initiate efforts to restore wider operations. |
|  | The incident lead will perform a formal handoff back to normal operations once DR objectives have been met. |
|  | A deactivation of the DR plan will be communicated, and a retrospective will be conducted to identify improvements. |

# Risk Assessments

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Hosting Provider | Service Component | Critical Service | Potential Risks | Likelihood | Impact | Resilience Strategy | Priority Sequence |
| Microsoft | Office 365 | Email, Documents | Service outages, Data breaches, Phishing attacks | Moderate | High | Multi-geo redundancy, Regular backups, MFA | High |
| Sage | Sage Payroll | Payroll Services | Data loss, Unauthorized access, Service downtime | Low | High | Regular backups, Role-based access control | High |
| SAP | ERP System | Business Operations | Data corruption, System failures, Cyber attacks | Moderate | High | High Availability, Regular backups, Patch management | High |
| Salesforce | CRM | Customer Management | Data breaches, Service interruptions, Unauthorized access | Low | High | Multi-region failover, Regular security audits, Data encryption | High |
| Amazon (AWS) | EC2 | Hosting | Server downtime, Data loss, Security breaches | Low | High | Auto-scaling, Snapshots, Security groups | High |
| Google | G Suite | Email, Documents | Service outages, Data breaches, Unauthorized access | Moderate | High | Geo-redundancy, Regular backups, MFA | High |
| Oracle | Oracle DB | Database Services | Data corruption, Unauthorized access, Service interruptions | Moderate | High | Data replication, Encryption, Regular backups | High |
| Intuit | QuickBooks | Accounting | Data loss, Unauthorized access, Service downtime | Low | Moderate | Regular backups, Role-based access control | Medium |
| Atlassian | Jira | Project Management | Service outages, Data breaches, Unauthorized access | Low | Moderate | Regular backups, Security patches, Data encryption | Medium |
| Dropbox | Cloud Storage | File Storage | Data loss, Unauthorized access, Service outages | Low | High | Multi-region replication, Encryption, Regular backups | High |
| Microsoft | Office 365 | Email, Documents | Service outages, Data breaches, Phishing attacks | Moderate | High | Multi-geo redundancy, Regular backups, MFA | High |

**Likelihood** is rated as:

* **High**: Event is expected to occur frequently.
* **Moderate**: Event might occur occasionally.
* **Low**: Event is unlikely to ever occur.

**Impact** is rated as:

* **High**: Event would have a serious impact on operations or would cause a significant financial loss.
* **Moderate**: Event would cause a noticeable disruption and require management attention.
* **Low**: The event would cause minimal disruption.

**Resilience Strategies**

* **High Availability**: Ensures that the service is distributed across different physical and virtual servers, reducing the chance of a single point of failure.
* **Backups**: Regularly scheduled backups that can be used to restore data to a point-in-time should data corruption or loss occur.
* **Multi-AZ Failover**: Utilisation of multiple availability zones within the same region to provide failover capabilities.
* **Geo-Redundancy**: Storing data in geographically diverse locations to protect against regional disasters.
* **Version Control & Backups**: Use of version control systems for code and infrastructure, combined with backups for critical configurations.
* **Dyno Redundancy**: In Heroku, dynos can automatically recover from hardware failures, and using more than one dyno can provide redundancy.
* **Platform's Built-in Redundancy**: Reliance on the inherent resilience and redundancy features provided by the platform (e.g., GitHub, CircleCI, Slack).
* **DNS Failover**: The capability to switch traffic from the failing site to a backup site in case of an outage.
* **Data Export**: Regular exports of data and reports to ensure that analytics data can be recovered in case of a loss of service.

Disaster Recovery Team

The following are the key staff that will co-ordinate the recovery of the services and report into the Disaster Management Team members.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Contact Details** | **Responsibilities** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Key External Contacts

The following are the contact details for any 3rd parties that may be needed in the event of execution of part or all of the DRP.

|  |  |  |  |
| --- | --- | --- | --- |
| **Organisation** | **Role** | **Contact Details** | **Comments** |
| ICO – Information Commissioner's Office (UK) | Legislative oversight of GDPR / DPA data | [Self-assessment & Reporting guide](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/)  **0303 123 1113** | To report any major breaches to sensitive personal data under GDPR / DPA |
| Insurance | Insurance Company |  | Details on insurance policy held here |
| Reliance ACSN | Cyber-attack response experts | <https://relianceacsn.co.uk/consulting/incident-response/> | Can offer support with how to approach major cyber attack issues (e.g. Ransomware, etc). |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Hierarchy of Notifications

The following summarises who will be responsible for contacting and communicating with whom in the event of a disaster.

# Comms Plan

## Contact list - Key Stakeholders

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Communication Method** | **Communication Owner** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Testing

|  |  |  |  |
| --- | --- | --- | --- |
| **Component** | **Testing Approach (paper / backup test / failover)** | **Date of last test** | **Instructions confirmed** |
|  |  |  |  |
|  |  |  |  |

# Document Maintenance

The Disaster Recovery Plan will be

To ensure the disaster recovery plan remains up-to-date, it will be reviewed and updated regularly as changes occur.

* The disaster recovery plan will be reviewed in full on an annual basis by the Head of Engineering.
* Any significant changes to systems, processes, or contracts should trigger a DR plan review.
* The following items will be reviewed for accuracy and updated as needed during DR plan maintenance:
  + Contact details for disaster recovery team members and key stakeholders
  + System inventory and architecture
  + Business impact analysis and risk assessments
  + Recovery procedures and instructions
  + DR invocation process
  + Testing schedule
  + Contracts and SLAs with vendors
  + Appendix documents like server specs, credentials, checklists
* The DR plan review will also be completed after any DR invocation, test, or change in recovery facilities to incorporate lessons learned.
* Any changes to the DR plan will be communicated to relevant stakeholders.

APPENDICIES

# Key Reference Materials

|  |  |
| --- | --- |
| **Description** | **Location** |
| Cyber Response Plan |  |
| Cyber insurance response policy |  |
| System Passwords and keys |  |

# Vendor SLA Agreements

# Important Information

|  |  |
| --- | --- |
| **Item** | **Note** |
| Passwords | Stored in LastPass? |
|  |  |
|  |  |

# Backup Summaries

|  |  |
| --- | --- |
| System |  |
| Owner |  |
| Risk Assessment |  |
| Backup Strategy |  |

# Recovery Procedures

Procedure A

|  |  |  |
| --- | --- | --- |
| Step | Action | Owner |
|  |  |  |
|  |  |  |

Procedure B

|  |  |  |
| --- | --- | --- |
| Step | Action | Owner |
|  |  |  |
|  |  |  |

Key Records & Contracts

|  |  |  |
| --- | --- | --- |
| Record | Primary Location | Alternative Location |
| Cyber insurance |  |  |