

**Business Continuity Toolkit**

**IT Disaster Recovery Plan Template**

*The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.*

Document review and approval

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Date | Revision |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

This document has been approved by

|  |  |  |
| --- | --- | --- |
|  | Approver name | Date approved |
|  |  |  |
|  |  |  |

**Contents**

[1 Purpose 3](#_Toc64618508)

[2 Scope 3](#_Toc64618509)

[3 Plan possession 3](#_Toc64618510)

[4 Key assumptions 3](#_Toc64618511)

[5 Business continuity roles and responsibilities 4](#_Toc64618512)

[6 Disaster recovery plan activation procedure 6](#_Toc64618513)

[7 Return to business-as-usual and subsequent activities 6](#_Toc64618514)

[8 Required communications 7](#_Toc64618515)

[9 Recovery Timeline & Resource Requirements 8](#_Toc64618516)

[10 Appendix 1 – forms and checklists 9](#_Toc64618517)

[11 Appendix 2 – prioritized business processes and RTOs 11](#_Toc64618518)

[12 Appendix 3 – contact information list 12](#_Toc64618519)

Purpose

The IT disaster recovery plan (DRP) serves as an aid to recovering technology systems which support critical business processes following a significant disruption. It contains information on how to recover the core network and each key technology system needed by business operations.

Scope

This IT DR Plan includes documented procedures to assist the IT DR Team to recover from a disruption of IT systems, ensuring the effective recovery of the organization’s key systems. This plan covers all key systems based on the dependencies captured in the business impact assessment (BIA).

Each technology resource supporting a critical business process has a combination of resilience measures to reduce the likelihood/impact of a significant disruption and recovery procedures to restore the technology functionality following a significant disruption. This plan focuses on the recovery procedures after a disruption occurs.

Plan possession

All personnel identified in section 5 as having disaster recovery responsibilities will have a copy of the latest version of this DRP through SharePoint access and either printed copies or digital copies on encrypted USB storage devices.

Key assumptions

1. Operational and cybersecurity incident response to protect IT assets and the technology environment will be addressed in separate plans. The DRP will be activated in case incident response activities are unable to recover systems within the defined period of time.
2. All personnel with DR responsibilities have been trained on the use of this DRP and have been given a copy of the latest approved version
3. Recovery procedures assume the worst-case scenario for the loss of the systems, i.e., that systems are not even partially available. Management personnel authorized to activate the DRP will have to determine whether to execute the full recovery procedures in the event the technology environment is partially available.

IT disaster recovery roles and responsibilities

The following roles are required to ensure successful activation and execution of DRP procedures:

| **Role** | **Responsibilities** | **Primary** | **Alternate(s)** |
| --- | --- | --- | --- |
| Management personnel authorized to activate the DRP | * Assesses the impact of a disruption and makes a decision on whether to activate DRP procedures as per section 6 * Informs the Business Continuity Coordinator that the DRP is being activated and which specific elements need to be executed. | *<Add>* | *<Add>* |
| Business Continuity Coordinator | * Once notified of DRP activation, begins issuing internal communications specified in section 8 * Liaises with the management team to determine whether the business continuity plan (BCP) needs to be activated, based on the severity of the technology disruption. | *<Add>* | *<Add>* |
| Communications Lead | * Issues all external communications specified in section 8. | *<Add>* | *<Add>* |
| DR Lead | * Maintains a record of decisions made and notable actions taken using the form in Appendix 1 * Reviews and approves deviations from DRP procedures and coordinate for management approvals on the spot * Oversees and leads the execution of the IT DRP * Issues regular communications to the Business Continuity Coordinator on the status of technology recovery efforts. | *<Add>* | *<Add>* |
| Disaster Recovery Team Members | Consists of IT personnel who execute/oversee the execution of recovery procedures for their technology areas. | *<Add>* | |
| External agencies / third parties | Third parties may be drawn upon to support organization’s IT disaster recovery efforts and have been identified in the specific procedures when their involvement is required. | *<Add>* | |

Disaster recovery plan activation procedure

Once incident response procedures are activated to the extent required to safeguard the organization’s technology environment, the authorized personnel listed in section 5 should inspect the specifics of the disruptive event to determine if it warrants activation of DRP procedures, including whether this is near the worst possible time for a disruption to occur and the anticipated downtime resulting from the event.

The DRP is typically activated as soon as the incident response activities determine that the recovery time is likely exceed the recovery time objectives agreed with business stakeholders.

See Appendix 3 for contact details for personnel authorized to activate the DRP.

Plan activation procedure:

1. Inspect the specifics of the disruptive event and its impact on the organization’s critical business processes to determine if it warrants activation of DRP procedures. Refer to Appendix 2 for a prioritized list of critical business processes and their associated recovery time objectives (RTOs), and specifically:
   1. If the disruption is expected to last for a period of time shorter than the RTO, no action may be required and incident response activities will continuite to resolve the disruption
   2. If the disruption is expected to last for a period of time longer than the RTO, consider executing recovery procedures for the impacted systems
2. Determine which DRP procedures (by system) need to be executed based on the severity of the loss and which critical business processes are impacted at the time of the disruption. This helps prioritize which systems to recover first. Refer to Appendix 2 for a prioritized list of critical business processes
3. Document the decision to activate DRP procedures using the template provided in Appendix 1
4. Notify the Business Continuity Coordinator that DRP procedures are being activated and to begin conducting the necessary communications as specified in section 8.

Note: subsequent to this approval, the situation may escalate and require additional DRP procedures to be activated. In that case, the decision-maker would follow this procedure again and expand the scope of the DRP procedures being executed.

Return to business-as-usual and subsequent activities

Once the cause of the disruption is addressed and the organization can return to its original (production) technology environment, the steps in section 10 will be executed to safely migrate key systems back to the main environment and minimize the risk of causing another disruption during the migration.

Once all systems are back to production, the DR Lead will inform the Business Continuity Coordinator to notify impacted stakeholders that the disruption situation is over. The DR Lead will also gather feedback on the effectiveness of DRP procedures and the overall process, and conduct a debrief meeting to document the lessons learned and capture any required improvements to organizations’ resilience and recovery measures. Any identified improvements will be integrated into an updated version of the DRP.

Required communications

1. Upon plan activation:
   1. The member of management authorizing DRP activation must notify the Business Continuity Coordinator and DR Lead of the activation and scope
   2. The DR Lead begins notifying Recovery Team Members with DR responsibilities that DRP procedures are required based on the scope of execution
   3. The Communications Lead issues a mass internal notification to all organization staff or subset of impacted staff notifying them of the DRP activation and any relevant instructions based on the procedures being executed
   4. The DR Lead provides Communication Lead with external notifications to relevant parties informing them of the disruption and that recovery procedures are underway
   5. The DR Lead communicates directly with any third parties that are part of the recovery team, such as managed services providers.
2. On-going communications during disaster recovery operations
   1. The Business Continuity Coordinator, with support from the DR Lead, will issue periodic status with updates and progress towards recovery of mission-critical systems to relevant stakeholders. The communications interval will be driven by the RTO of the impacted resources at the discretion of the Business Continuity Coordinator, e.g., hourly status updates for a resource with an RTO of 24 hours or daily status updates for a resource with an RTO of 1 week
   2. The Business Continuity Coordinator, with support from the DR Lead, will issue separate status updates to organization’s management at the same frequency, including a copy of the decisions-made form and any additional relevant details on recovery progress
   3. Additional communications may be issued by the Business Continuity Coordinator (internally) and the Communications Lead (internally/externally) throughout recovery and temporary operations, as required.
3. At the conclusion of a disruption:
   1. The DR Lead will inform Business Continuity Coordinator or the Communications Lead who at their end will inform internal stakeholders that the disruption situation is over, and the Communications Lead will do the same for external parties
   2. The DR Lead will also gather feedback from relevant stakeholders on the effectiveness of DR procedures and the overall process and provide it to Business Continuity Coordinator.
4. The following hierarchy of communications will be followed:
5. Communications channels:
   1. Acceptable communications channels include: in-person, phone-call, text message, corporate email or MS Teams chat, depending on availability
   2. Email is preferred for mass notifications, if available, followed by text messages
   3. Phone-call or in-person communication is preferred for notifications that require confirmation, e.g., to confirm that the person being notified received the message and will execute their DRP procedures.

Recovery procedures

This section contains the recovery procedures for the technology environment(s) which support critical business processes. The systems are ordered by time-sensitivity (RTO), starting with the shortest recovery timeframes.

The DR Lead will maintain a record of decisions made and notable actions taken using the form in Appendix 1, and review and approve deviations from DRP procedures and pre-approved activities/spending.

The recovery begins with recovering the core network and infrastructure, ensuring all cybersecurity safeguards and tools are in place, before starting to recover individual systems.

**Core network infrastructure recovery**

|  |  |
| --- | --- |
| **Network and connectivity** | |
| **Recovery procedures** | *<Add>* |
| **Security controls and tools** | |
| **Recovery procedures** | *<Add>* |
| **Basic server infrastructure** | |
| **Recovery procedures** | *<Add>* |

**Cloud infrastructure recovery**

|  |  |
| --- | --- |
| **Network and connectivity** | |
| **Recovery procedures** | *<Add>* |
| **Security controls and tools** | |
| **Recovery procedures** | *<Add>* |
| **Basic server infrastructure** | |
| **Recovery procedures** | *<Add>* |

**<System #1> recovery procedures**

|  |  |
| --- | --- |
| **Application recovery steps** | *<Add>* |
| **Database recovery steps** | *<Add>* |
| **Functionality testing steps** | *<Add>* |

Wind-down and return-to-normal procedures

Once the cause of the disruption is addressed and the organization can return to its original (production) technology environment, the following steps will be executed to safely migrate key systems back to the main environment and minimize the risk of causing another disruption during the migration.

|  |  |
| --- | --- |
| **Network and infrastructure readiness steps** | *<Add>* |
| **Security safeguards readiness steps** | *<Add>* |
| **System migration steps** | *<Add>* |
| **Functionality testing steps** | *<Add>* |

Appendix 1 – forms and checklists

**DRP activation decision and scope form:**

|  |  |
| --- | --- |
| **Date and time** |  |
| **Details of the disruptive event** |  |
| **Expected duration of the disruption** |  |
| **Impacted critical business processes** |  |
| **DRP procedures required (list the environments and systems for recovery procedures to be activated)** |  |
| **Name(s) of personnel authorizing DRP activation** |  |

**Decisions-made, actions taken and subsequent events form:**

|  |  |
| --- | --- |
| **Key decisions made post plan activation** |  |
| **Key actions taken per the approved recovery procedures, and any approved deviations from the plan** |  |
| **Communications issued (internal and external)** |  |
| **Notable subsequent events that occurred during the disruption** |  |

Appendix 2 – prioritized business processes and RTOs

The following table outlines the organization’s business processes that reach an impact rating of ‘4-High’ within the assessed timelines. Impact ratings for all business processes can be found in the detailed BIA workbooks.

| **Department** | **Process name** | **Recovery time objective** | **Technology dependencies** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Appendix 3 – contact information list

| **Name** | **Organization** | **Phone number(s)** | **Email address** |
| --- | --- | --- | --- |
|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |