Disaster Recovery Playbook

CyberAlberta

June 3rd, 2024

Contact Information:
Cybersecurity Division
Technology and Innovation
5th floor, Terrace Building
9515 – 107 ST NW
Edmonton, AB T5K 2C1

Published by:
Technology and Innovation, Cybersecurity Division

CYBER ALBERTA

PREFACE

This document is a generic playbook based on the Government of Alberta's Disaster Recovery standard operating procedure. You can use this document to construct your own organization's disaster recovery playbook or process. References to internal teams or policy instruments have been encapsulated in brackets ("< >"). These should be replaced with information specific to your organization. For more information, please contact the CyberAlberta general mailbox:

CyberAlberta Support
cyberalberta@gov.ab.ca

Business continuity events

Anyone identifying a potential disaster should report it immediately to <your organization's Service/Help Desk>, per the <your organization's Major Incident Response Process>, where the incident will be tracked and managed.

Note: This page can be excluded or re-written to be a preface tailored to your organization.

Effective Date

This publication takes effect on DATE, 2024.

Approved by: Martin Dinel	**Owner:** CyberAlberta (Martin Dinel, ADM)	
Approval date: May 28th, 2024	**Reviewed date:** May 28th, 2024	**Next review date:** May 28th. 2025
Contact: Martin Dinel, ADM for the Cybersecurity Division Email: martin.dinel@gov.ab.ca	**Policy Instrument type:** Playbook	

TABLE OF CONTENTS

OVERVIEW

The **IT disaster recovery playbook** is a subset of the organization's business continuity plan (BCP) which encompasses IT and non-IT aspects of business resumption such as facilities, personnel, and communications.

The IT disaster recovery playbook outlines a series of procedures and protocols designed to help organizations effectively respond to different types of IT disasters and coordinate the resumption of IT services.

Disasters can include natural events like hurricanes, earthquakes, floods, human induced events such as cyberattacks, data breaches, human error, or infrastructure failures. The playbook outlines steps to be taken during and after a disaster to ensure the continuity of operations and the rapid restoration of services.

Benefits of having a DR Playbook:

Standardization: A playbook provides a standardized set of procedures for responding to disasters. This ensures that all members of the organization understand their roles and responsibilities during a crisis, reducing confusion and improving response efficiency.

Rapid Response: With predefined steps and protocols in place, teams can act quickly and decisively when a disaster occurs. This can minimize downtime, reduce data loss, and mitigate the impact of the disaster on the organization's operations.

Risk Management: By identifying potential risks and outlining mitigation strategies in advance, a disaster recovery playbook helps organizations proactively manage and mitigate risks. This can include measures such as data backups, redundancy planning, and security protocols to protect against cyber threats.

Compliance and Regulation: Many industries have regulatory requirements for disaster recovery planning and preparedness. A playbook ensures that the organization remains compliant with these regulations and can provide evidence of preparedness in case of audits.

Training and Preparedness: Regularly reviewing and updating the playbook offers an opportunity for training and preparedness exercises. This ensures that all stakeholders are familiar with their roles and responsibilities and are prepared to respond effectively in a crisis situation.

Confidence and Resilience: Knowing that there is a well-defined plan in place can boost confidence among employees, customers, and stakeholders. It proves that the organization is prepared to handle disaster events and can recover quickly from disruptions, thereby enhancing resilience and reputation.

The disaster recovery playbook is a vital resource for organizations, aiding in thorough preparation for and swift response to disaster scenarios and events. By establishing robust disaster recovery protocols, businesses ensure continuity and limit the adverse effects of emergencies to their operations.

This document outlines the three phases in preparing for and responding to an IT disaster event:

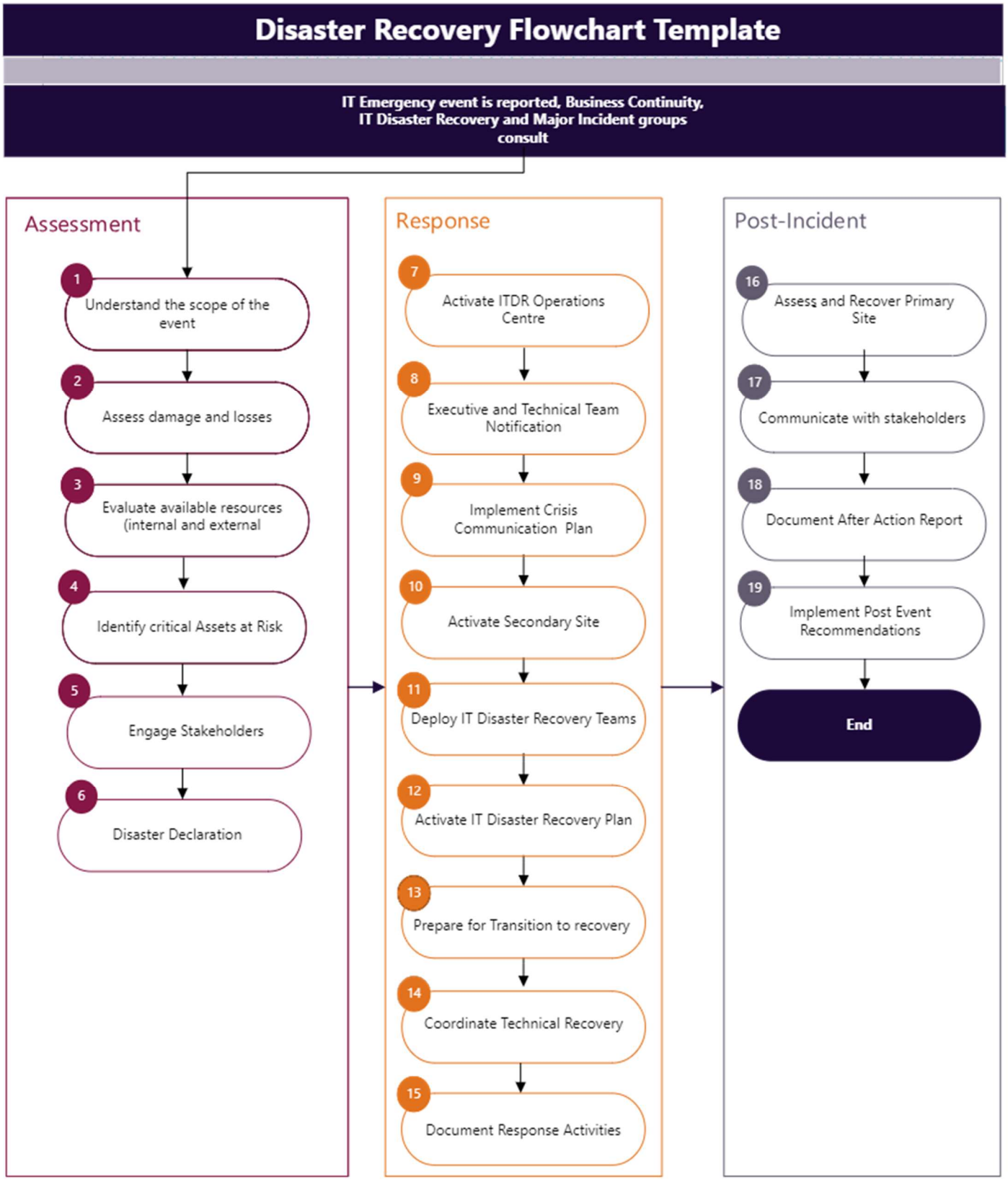
1. Assessment
2. Response
3. Post-Incident

If you are witnessing a disaster event, whether it is in progress or has already occurred, here are steps you should take:

1. **If life safety is a concern, or this is a community disaster, contact emergency services.**
2. **If this is a facility event, activate <your company's> Facility Emergency Response Plan (FERP)**
3. **If this is an IT related event, contact <your Service/Help Desk contact information> Service/Help Desk.**

For more information on all cybersecurity-related topics please email <your cybersecurity department mailbox>

Disaster Recovery Flowchart Template



ASSESSMENT

Once an IT incident or major incident has been reported, it enters the assessment phase. Key activities that occur during the assessment phase include, but are not limited, to the following:

Activity	Actions
1	☐ **Understand the scope of the event.** ○ Assess the nature and magnitude of the disaster: Determine the type of disaster (natural, technological, human induced, etc.) and its severity. ○ Identify affected areas: Determine the extent of the disaster and the areas impacted. ○ Work with Facilities to understand scope and magnitude of affected infrastructure if affected. Perform assessment to understand scope of disaster on IT systems, infrastructure, and data.
2	☐ **Assess damage and losses.** ○ Determine the extent of loss, especially for critical systems and applications: assess damage to critical infrastructure (server, storage, network, etc.). ○ Determine the expected duration of the disaster and the resources required for recovery efforts. ○ Estimate duration and recovery efforts.
3	☐ **Evaluate available resources** (internal / external) ○ Assess internal resources: Evaluate availability of personnel, equipment, facilities, supplies and backups within the organization that can be mobilized for disaster response and recovery. ○ Identify external resources: Identify vendors, partners, and contractors required to support recovery efforts. ○ Conduct resource mapping: Create comprehensive inventory or map of available resources, capacity, and availability, to facilitate efficient allocation and utilization during disaster response and recovery efforts. ○ Identify deficiencies or limitations that may impact recovery efforts.
4	☐ **Identify critical assets** ○ Review critical IT services / application recovery objectives (recovery time objective-RTO, recovery point objective-RPO) factoring in business cycle, seasonal implication, regulatory compliance, etc. ○ Identify critical IT infrastructure: Including server, storage, network, database, etc. available. ○ Physical infrastructure: including building access, security, and access control systems.
5	☐ **Engage stakeholders** ○ Notify the organizations senior management, Communications, internal/external stakeholders accordingly. ○ Customize existing communication artifacts to address the current situation.
6	☐ **Disaster declaration** ○ Senior management Team initiates disaster declaration. ○ Notification of disaster declaration: Notify all respective teams (e.g. infrastructure, application, and business) of disaster declaration. ○ Confirm scope of recovery, priority, and next steps.

By conducting these key activities during the assessment phase, organizations can gain a comprehensive understanding of the disaster's impact and mitigate its effects and restore normal operations.

Essential communications during the assessment phase of a disaster event can include:

Timing	From	To	General Message
Declaration of disaster event.	Cybersecurity	Senior Management Corporate Communication Stakeholders IT Staff	Immediately notify stakeholders, IT staff, management and other key personnel using established distribution lists. Use established communication channels to ensure prompt notifications. Communications should include protocols for proactive and reactive communications to ensure critical information is received by the appropriate target(s) as efficiently and accurately as possible. Use pre-existing templates and processes for DR communications efforts to ensure these objectives are met.
Status updates	Cybersecurity	Senior Management Corporate Communication Stakeholders IT Staff	Provide Regular status updates on the assessment progress to keep all parties informed about the current situation. Include details about the extent of the damage, affected systems and initial findings from the assessment.
In response to multiple public concerns or media inquiries	Communications	Public	High-level messaging noting that service impacts are being investigated and thanking clients for their understanding. At this stage, public communications should remain reactive. Avoid sharing undetermined information, including details about the disaster event and restoration timelines. Messaging should be approved by appropriate members of cybersecurity and senior management. Responding to public comments can help control the narrative and reduce speculation.

RESPONSE

There are several key activities to the response phase when dealing with a disaster event, with the main goal being to recover from the incident in the least amount of time possible:

Activity	Actions
7	☐ **Activate IT Disaster Recovery (ITDR) Operations Centre** ○ Activate ITDR Emergency Response Team: Incident Commander, IT Disaster Recovery Coordinator, Business Continuity Liaison, Communications, Logistics, Finance, Admin, etc... ○ Establish ITDR Operations Centre: Set up physical or virtual command centre to serve as focal point for coordinating and directing response activities.
8a	☐ **Technical Team Notification** ○ Notify the technical teams as soon as a disaster event is confirmed using established communication channels. Include details of the event, including affected systems, data, and infrastructure. ○ Establish next steps: Maintain on going communications with technical teams to provide situational awareness, communication channel(s), timing, etc.to begin response activities. ○ Ensure the technical teams have access to any necessary resources tools and support required.
8b	☐ **Executive Team Notification** ○ Immediate notification to senior management as soon as disaster is declared. ○ Executive briefing: Include event synopsis, immediate assessment, planned response, recovery strategy and timings.
9	☐ **Implement Crisis Communication Plan** ○ Activate communication plan: Establish communications channels / modalities with internal and external stakeholders, including staff, vendors, suppliers, and partners. ▪ Ensure stakeholders are kept informed. ▪ Minimize misinformation. ▪ Maintain confidence in the organization's ability to manage the situation.
10	☐ **Activate Secondary Site** ○ Implement the recovery plans. ○ Establish start time for all teams to begin based on DR Plan. ○ Confirm personnel shift, transition, and communication schedules.
11	☐ **Deploy IT Disaster Recovery Teams** ○ Activate recovery teams ○ Coordinate resource allocation: Coordinate the allocation and deployment of personnel to support recovery operations. ○ Review recovery priorities, strategy and activities according to established procedures and timelines. ○ Keep stakeholders informed of status of recovery progress
12	☐ **Activate IT Disaster Recovery Plan** ○ Execute Recovery Plan: Implement the predefined recovery procedures outlined in the disaster recovery plan to restore critical systems, operations, and infrastructure to minimize downtime and mitigate the impact of the disaster on business operations.
13	☐ **Prepare for Transition to Recovery** ○ Establish start time for all teams to begin. ○ Confirm personnel shift, transition, and communication schedules. ○ Provide updates to recovery prioritization if it deviates from the plan. ○ Confirm recovery systems readiness status to restore data and applications at the secondary / recovery site. ○ Set up a monitoring system to document restoration activities in accordance with the plan.

Activity	Actions
	○ Be prepared to adapt plans and strategies to address risks or emergent circumstances.
14	☐ **Coordinate Technical Recovery** ○ Activate collaboration / communication channel(s) for various stakeholder teams to effectively coordinate recovery (technical, senior management, etc.). ○ Coordinate recovery activities with response teams (internal / external). ○ Follow predefined recovery process / procedures. ○ Re-prioritize recovery efforts based on emergent situations. ○ Validate the integrity and reliability of recovery environment as services are restored. ○ Escalate critical issues to appropriate levels of management for immediate support.
15	☐ **Document Response Activities** ○ Document all recovery activities, including task completion, problems / challenges encountered, and decisions made. ○ Document changes to system configurations, disaster recovery plans, and standard operating procedures, to reflect any changes made during the recovery process. ○ Update recovery plans and documentation based on the findings and any lessons learned from recovery process to improve the effectiveness and efficiency of future recovery operations. ○ Task teams to keep detailed logs for future analysis and improvement.

By Effectively managing these key activities during the recovery phase, organizations can minimize the impact of IT disasters and restore operations in a timely manner, mitigating potential losses and ensuring business continuity.

Essential internal and stakeholder communications during the response phase of disaster event can include:

Timing	From	To	General Message
After initial assessment is completed and initial communication occurred	Cybersecurity	IT Support Teams Senior management	Promptly notify all relevant stakeholders, including IT staff, management, and affected users, about the disaster event and the activation of the response phase. Clearly communicate the nature and severity of the incident.
Routinely	Cybersecurity	Senior management Stakeholders IT Staff	Provide regular updates on the status of response activities to keep stakeholders informed about progress, challenges, and achievements. Use various communication channels such as email, instant messaging, conference calls, and status reports to disseminate updates effectively.
When required	Cybersecurity	Communications Team	If your organization has a communications team, they may be able to support stakeholder, internal, and public communications. Ensure communications is aware of high-level updates, as they may impact messaging. Public communications materials and approach should be approved by appropriate members of cybersecurity and senior management. Facilitate Executive decision-making by providing relevant information, analysis, and recommendations to decision-makers. Ensure that

Timing	From	To	General Message
			decision-makers have access to real-time updates and insights to make informed decisions quickly.

Depending on the severity of the disaster event, essential public communications during the response phase of a disaster event can include:

Timing	From	Tactic	General Message
Upon notification	Communications	Communications plan Key messages	Outline the overall communications approach for stakeholders, staff, and the public. Develop key messages that share the most important pieces of information with the audience to help keep messaging consistent. Consider timing and messaging. Be transparent without sharing sensitive information. The plan and messaging should be approved by appropriate members of cybersecurity and senior management.
In response to public inquiries	Communications	Social media	Provide high-level updates to keep clients informed on the situation. Responding to public comments can help control the narrative and reduce speculation. Individuals will often go to social media when experiencing a technical issue. Avoid sharing sensitive or undetermined information, including restoration timelines. Depending on the level of public impact, consider whether a reactive or proactive approach is most appropriate. Reactive may be more suitable when public impacts are minimal, whereas proactive may be more suitable for larger incidents.
In response to media inquiries	Communications	Media statement or response Web content Direct stakeholder communications	Provide relevant information about the incident. Consider creating library of media questions and responses to ensure consistent messaging is shared with all inquirers. The disaster event results in significant public impacts, inform stakeholders of the incident and steps being taken to resolve the situation. Use existing channels and, if required, provide multiple updates. This will help reduce speculation and assure clients they are being considered during response. Be transparent without sharing sensitive information. Avoid undetermined information, including restoration timelines. It should be

Timing	From	Tactic	General Message
			approved by appropriate members of cybersecurity and senior management.

POST INCIDENT

After an IT disaster event, several key activities are necessary to ensure effective recovery and restoration of operations. These activities aim to assess the impact of the disaster, prioritize recovery efforts, and implement measures to prevent and mitigate future incidents. Revising the Incident Response Plan based on these lessons learned will ensure that the organization has the most robust response and recovery plans possible. These lessons learned may also be shared through secure channels with other organizations, such as the Cyber Alberta Community of Interest, as sharing these lessons can benefit other organizations and the cybersecurity community, ensuring greater all-around protection for Albertans.

Key activities of the post-incident phase include, but are not limited to:

Activity	Actions
16	☐ **Assess and Recover to Primary Site** ○ Assess primary site readiness for recovery to operation, including facility systems, IT infrastructure, server, storage, network, etc. ○ Verify the effectiveness of data replication mechanisms between the primary and secondary sites to ensure data consistency and integrity. ○ Validate recovery procedures and timing. ○ Assess resource availability and schedule. ○ Initiate defined process / procedures to recover core infrastructure services and applications to the primary data centre.
17	☐ **Communicate with Stakeholders** ○ Communicate with key stakeholders: Include senior management, IT staff, vendors, and business units, to coordinate recovery efforts and address any concerns or dependencies related to the failback process.
18	☐ **Document After-Action Report (AAR)** ○ Gather information: Collect data, incident reports, problem logs, and documentation related to the IT disaster event, including timelines, decisions made, actions taken, and outcomes. ○ Evaluate response actions: Assess the effectiveness of response actions taken during the IT disaster event, including incident detection, escalation, containment, mitigation, communication and recovery. ○ Analyze outcomes: Analyze the outcomes and impacts of the IT disaster event, including disruptions to IT services, data loss, financial implications, and reputational damage. ○ Identify strengths and weaknesses: Identify strengths and weaknesses in the IT response effort, including strengths to be reinforced and weaknesses to be addressed through corrective actions or improvements in IT disaster recovery plans and procedures. ○ Document lessons learned: Document key lessons learned from the IT disaster event, including technical insights, operational challenges, root causes of failures, and opportunities for improvement in IT infrastructure, systems, and processes. ○ Develop recommendations: Formulate actionable recommendations based on the findings of the after-action report, including specific measures to enhance IT resilience, improve incident response capabilities, and mitigate future IT disaster risks. ○ Prioritize actions: Prioritize recommended actions based on their potential impact, feasibility, and urgency, and develop an implementation plan outlining responsibilities, timelines, and resources required for each action. ○ Share findings: Share findings, recommendations, and lessons learned from the after-action report with relevant stakeholders, including senior management, technical teams, and business units, to promote transparency, accountability, and continuous improvement in IT disaster preparedness and response efforts.
19	☐ **Implement Post Event Recommendation** ○ Update recovery processes, strategies, plans and documentation based on the findings and any lessons learned from recovery process to improve the effectiveness and efficiency of future failback operations.

Activity	Actions
	○ Monitor progress: Implement and monitor recommended actions and track progress towards addressing identified deficiencies and improving IT resilience. ○ Periodically review the after-action report as needed to reflect ongoing efforts and emerging insights.

Essential communications during the post incident phase of a disaster event can include:

Timing	From	To	General Message
After the incident has been resolved	Cybersecurity	Senior management	Post incident report. A report that documents the incident fully, plans for recovery (if required), Identify any needs for downstream communication, and lessons learned.
After post-incident report has been communicated to senior management	Cybersecurity and Senior management or Communication team	Clients/stakeholders/employees	Notify all relevant stakeholders, including employees, customers, suppliers, and regulatory bodies, about the incident. Provide clear and concise information about the nature of the incident and its impact.
After Post-incident report has been communicated to senior management and stakeholders.	Communications	Media/public if it makes sense for the organization	Coordinate communication with the media and external stakeholders to manage the organization's public image and reputation. Provide accurate and timely updates to prevent the spread of misinformation and address concerns from the public.

APPENDIX

REFERENCES

Disaster recovery plans are essential safeguards to ensure the recovery of critical data, IT systems and networks in any Disaster scenario. These plans play a crucial role in enabling organizations to maintain their business objectives during disruptions keeping the business operational.

Disaster recovery plans are designed to protect and mitigate infrastructure and systems against a disruptive event. The financial implications of such disruptions can be substantial.

Disaster Recovery Resources

Cybersecurity | NIST

Disaster Recovery Institute Canada

Canadian Centre for Cyber Security

DATA CENTRE CRITERIA BEST PRACTICES

When evaluating data center options, its essential to understand the specific features, certifications and service level agreements offered by each provider to determine if they meet your business requirements for reliability, security, and availability. All data centres should keep up with regular maintenance and be subject to inspections. Keep in mind that a data centre in a shared building is at the mercy of other tenants.

Recommendations for a data centre:

Redundant components: Data centres and IT infrastructure may have redundant components for power, cooling, and network connectivity to ensure high availability and minimize downtime to ensure consistent availability of services.

24/7 Monitoring and support: Typically have 24/7 monitoring and support to promptly address any issues or emergencies.

Physical Security measures: Robust physical security measures in place, including access controls, fire suppression, surveillance systems and security personnel to protect against unauthorized access and breaches.

Disaster Recovery and Business Continuity: Disaster recovery and business continuity plans in place to minimize the impact of an event.

DISASTER PREPARATION

Key activities to prepare for a disaster include:

Risk assessment and Analysis: Identify potential threads and vulnerabilities to IT systems and infrastructure. Assess the potential impact of various disaster scenarios on critical operations, systems and data.

Business Impact Analysis (BIA): The outcome of a Business Impact Analysis (BIA) is a comprehensive understanding of the potential impacts of disruptions on business operations and the organization as a whole. Specifically, the BIA identifies and prioritizes critical business functions, processes, and resources, as well as the dependencies and interrelationships between them. Based on the identified impacts, the BIA establishes recovery

priorities and recovery time objectives (RTO/RPO's) for critical business functions and resources, guiding the development of disaster recovery and business continuity plans.

Develop a Disaster recovery Plan (DRP): Create a comprehensive plan outlining the steps to be taken in response to various disaster scenarios. Define roles and responsibilities, establish communications methods and mediums, identify resources needed for recovery.

Testing and training: Regulary test the effectiveness of the disaster recovery plan through conducting of tabletop, functional or full scale disaster recovery exercises and drills. Testing trains and reinforces employees on their roles and responsibilities during a disaster and makes sure they understand the process and procedures outlined in the DRP.

Vendor and Partner collaboration: Collaborate with vendors, service providers and partners to ensure they have adequate disaster recovery measures in place. Review service level agreements (SLAs) and make sure they include provisions for disaster recovery and business continuity.

Documentation, Documentation and more Documentation: Document all aspects of the disaster recovery plan, including procedures, configurations, contacts, vendors. Keep this documentation up to date and accessible to stakeholders.

Continuous Improvement: Regularly review and update the DRP based on changes in technology, business requirements and infrastructure. Incorporate lessons learned from past incidents and test results to enhance preparedness.