DISASTER RECOVERY INFORMATION TECHNOLOGY POLICY

Policy Code:	**TM7**
Version:	**2**
Approved by:	**The Board**
Approval Date:	**11/04/2024**
Decision Number:	**B.01.2024.07**

Table of Contents

1. Introduction

The Disaster Recovery Policy outlines the framework to ensure the continuation of vital business processes in the event that a disaster does occur, by providing an effective solution to recover all these business processes within the required timeframe, using secure records that are stored off-site. The recovery strategy for alternate processing includes the 'Hot-Site' and the alternatives available if the primary location is not available to provide disaster recovery services for the various system environments.

The Da Vinci Institute requires adequate protection to be in place to assure the continuity and recovery of the institution's business following the loss of technology systems. This policy defines the requirements for a baseline Disaster Recovery Plan to be developed and implemented that will describe the processes to recover Information Technology (IT) systems, applications and data from any type of disaster that causes a major outage.

The Disaster Recovery Policy outlines the processes to handle high-level coordination activities surrounding any crisis situation regarding information technology. The term 'disaster' is relative as disasters can occur in varying degrees.

The aim of the disaster recovery strategy is to ensure that every reasonable measure has been taken to re-inforce recovery capability and to identify and mitigate potential risks that exist within the processing environment as risk avoidance is a critical element in the disaster recovery process.

2. Definitions

Term	Definition
Disaster	Any event that can cause a significant disruption in operational and/or computer processing capabilities for a period of time, which affects the operations of the business. The purpose of defining a crisis or a discontinuity is to establish a documented description of what constitutes a crisis or a discontinuity. The intent is to minimise the decision-making process when an event occurs
Disaster Recovery System	The on-going process of planning, developing, testing and implementing disaster recovery procedures and processes to ensure the efficient and effective resumption of vital business functions in the event of an unscheduled interruption

Term	Definition
Hot Site	Is a commercial disaster recovery service that allows a business to continue computer and network operations in the event of a computer or equipment disaster. If an enterprise's data centre becomes inoperable, that enterprise can move all data processing operations to a hot site
Recovery Time	The duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity
Recovery Point Objective (RPO)	How old the data will be once the systems are recovered
Recovery Time Objective (RTO)	The length of time a business can be without data processing availability
Cloud-Based	Cloud-Based: Deployment model where software, applications, and IT resources are hosted and accessed over the internet through remote servers provided by a third-party cloud service provider. Offers scalability, flexibility, and reduced hardware management, with pay-as-you-go pricing based on usage
On Premises (On-Prem)	On-Premises (On-Prem): Traditional deployment of software or IT infrastructure within an organisation's physical premises or data centers, offering control, security, and customization. Requires upfront capital investment and ongoing maintenance

3. Legislative Context

The Disaster Recovery Policy is benchmarked against, and should be read in the context of the following Acts, legislative guidelines and Da Vinci policies:

i. Companies Act No. 71 of 2008
ii. Higher Education Act No. 101 of 1997 as amended 2003.

Da Vinci Policies:

iii. Acceptable use of Information Systems
iv. Communication and Media
v. Electronic Information and Communication System
vi. Firewall
vii. Incident and Service Management Information Technology

viii. Information Security
ix. Language
x. Privacy and Confidentiality
xi. Records and Administration Management
xii. Reputational Risk
xiii. Wireless Communications.

4. Scope

The Disaster Recovery Policy is directed to the IT Management Staff who is accountable to ensure the Disaster Recovery Plan is developed, tested, kept up-to-date, and to provide information for the handling of a crisis situation for the following parties:

4.1. Executives.
4.2. Legal team.
4.3. Finance Department.
4.4. Investor Relations.
4.5. Corporate Communications.
4.6. Corporate Administration.
4.7. Marketing and Sales.
4.8. Human Resources.
4.9. Technology Management.
4.10. Academic Management.

5. Disaster Recovery Plan Objectives

5.1. The Disaster Recovery Plan is designed to ensure the continuation of vital business processes in the event that an emergency or crisis situation should occur at any of the business locations to control all activities associated with a crisis situation in a pro-active manner, and to lessen the potential negative impact with the media, the public and with shareholders. This plan should be updated annually and should always be readily available to authorised personnel to:

5.1.1. Respond effectively in a crisis situation.
5.1.2. Manage the crisis in an organised and effective manner.

5.1.3. Limit the magnitude or impact of any crisis situation to the various business units.

5.2. The Disaster Recovery Plan addresses the following issues:

5.2.1. The plan for technology recovery in the event that a disaster should strike data processing centre(s).

5.2.2. Issues surrounding the business operations and business units should a disaster affect the business operations.

6. Elements Of Disaster Recovery Process

6.1. The disaster recovery process consists of the following elements:

6.1.1. Critical Application Assessment

6.1.2. Back-Up Procedures

6.1.3. Recovery Procedures

6.1.4. Implementation Procedures

6.1.5. Test Procedures

6.1.6. Plan Maintenance.

6.2. Disaster Recovery Plan activities are initiated by a situation or crisis alert procedure. After discovery of an incident, the Disaster Recovery Team will perform an assessment of the situation and determine if there is a need to declare an emergency or crisis and activate the Disaster Recovery Plan.

6.3. Once the plan is activated, assigned management personnel will be alerted and directed to activate their specific procedures.

6.4. An outage (crisis/discontinuity) may exist when:

6.4.1. A service providing support to a critical business function fails.

6.4.2. It is determined that the service cannot be restored before the point when it becomes vital to the business.

7. Disaster Recovery Incident

7.1. The disaster recovery scenario that will be specifically addressed within the scope of this policy is the loss of access to the computer centre and the data processing capabilities of those systems and the network connectivity addressing the recovery of the critical systems and essential communications.

7.2. The disaster scenario assumes that all equipment in the computer room is not salvageable, and that all critical telecommunications capability has been lost.

7.3. In the event of a declared disaster, key personnel will take immediate action to alert the parties affected by the disaster

7.4. Restoration of the critical coverage will be provided after a disaster is declared, and after turnover of the disaster recovery backup site.

7.5. Restoration will include, without limitation, the following:

7.5.1. Delivery of the authorised user data and software archived in off-site storage to the Information Technology Disaster Recovery Centre.

7.5.2. Connecting network lines to the Disaster Recovery Centre.

7.5.3. Operating the Critical Applications on the configuration at the Disaster Recovery Centre.

7.5.4. Provide critical coverage at the Disaster Recovery Centre.

7.5.5. Provide workspace and required equipment.

8. Recovery Strategy

8.1. The recovery strategy as part of the Disaster Recovery Plan will be to relocate critical information systems processing to an alternate computer-processing centre at the Hot-Site (Disaster Recovery Services provider).

8.2. The Disaster Recovery Services provider is responsible for ensuring that the system configurations and the associated network requirements are accurate and technically feasible at all times.

8.3. Annual testing will be a part of the alternate processing strategy.

9. Recovery Phases (Cloud-based and on premises (On-Prem)

9.1. **On-Prem:** Recovery activities will be conducted in a phased approach. The emphasis will be to recover the critical applications effectively and efficiently. Critical applications will be recovered over a period of time after data centre activation.

Cloud Based: Recovery activities will be conducted in a phased approach within our cloud environment. The emphasis will be to recover the critical applications effectively and efficiently. Critical applications will be restored over a period of time after initiating the cloud recovery process.

9.1.1. **Phase I (On-Prem)**

Operations are moved to the Disaster Recovery Back-up Site and the Emergency Operations Centre. There is a period of up to 24 hours allowed for organisation of and the turnover of the disaster recovery backup site.

9.1.2. **Phase II (On-Prem)**

Recover critical business functions, restoration of the critical applications and critical network connectivity. The goal is to recover the systems and network to enable customers to continue business.

9.1.3. **Phase III (On-Prem)**

Return data processing activities to the primary facilities or another computer facility.

9.1.4. **Phase I (Cloud-based)**

Verify the integrity and availability of backup data within the cloud environment. Ensure that all critical data and configurations are up to date and readily accessible for recovery. Prepare the cloud-based disaster recovery environment, ensuring that necessary resources are available, and network connectivity is established.

9.1.5. **Phase II (Cloud-based)**

Restore critical business functions by deploying the required applications and services within the cloud environment. Focus on achieving functional recovery to enable customers to resume business activities. Verify the functionality of restored applications and conduct necessary testing to ensure proper operation within the cloud environment.

9.1.6. **Phase III (Cloud-based)**

Validate the cloud-based recovery setup and conduct any required optimizations to meet performance and security standards.
As our operations run within a cloud environment, the recovery approach offers the advantage of flexibility and accessibility. This allows employees to work from anywhere, anytime, and from anyplace, ensuring uninterrupted business continuity. Regularly review and update the cloud-based recovery plan to align with changes in the organization's cloud infrastructure and critical applications.

9.2. The following conditions, if met, will constitute a successful recovery effort:

9.2.1. Restore critical applications to the most current date available on backup tapes stored off-site.

9.2.2. Updating the systems and databases will take place as the recovery effort progresses as response times will probably be slower than normal production situations.

9.3. The recovery procedures consist of recovery at the present data centre site after repairs have been made, or at the disaster recovery backup site and the emergency operations centre. It also includes recovery procedures for the restoration of critical applications using either data recovered from the damaged data centre, or from the back-up data stored off-site.

10. Objectives Of The Disaster Recovery Plan

10.1. The Disaster Recovery Plan provides a state of readiness allowing prompt personnel response after a disaster has occurred to provide for a more effective and efficient recovery effort to:

10.1.1. Limit the magnitude of any loss by minimising the duration of a critical application service interruption.

10.1.2. Assess damage, repair the damage, and activate the repaired computer centre.

10.1.3. Recover data and information imperative to the operation of critical applications.

10.1.4. Manage the recovery operation in an organised and effective manner.

10.1.5. Prepare technology personnel to respond effectively in disaster recovery situations.

10.2. Disaster Recovery Plan activities are initiated by a situation or disaster alert procedure.

10.3. After the discovery of an incident, technology management will be informed of a potential disaster at the computer processing centre.

10.4. The Recovery Management Team will perform an assessment of the situation and determine if there is a need to declare a disaster and activate the Disaster Recovery Plan.

10.5. Once the Plan is activated, assigned recovery personnel will be alerted and directed to activate the recovery procedures they are responsible for.

11. Recovery Objectives

11.1. Recovery of applications and customers that are critical to the business and the Identification of the Recovery Time Objective (RTO), and the Recovery Point Objective (RPO).

11.2. Recovery objectives should be reviewed and updated by management on an annual basis.

12. Disaster Recovery Plan Elements

The plan contains of the following elements:

12.1. Scope and Objectives.

12.2. Business Recovery organisation and responsibilities (Recovery Team).

12.3. Major Plan Components - format and structure.

12.4. Scenario to execute plan.

12.5. Escalation, Notification and Plan Activation.

12.6. Vital Records and Off-Site Storage Programme.

12.7. Personnel Control Programme.

12.8. Data Loss Limitations.

12.9. Plan Administration (general).

13. Disaster Recovery Plan

13.1. The purpose of the plan is to define the activities necessary to maintain the Disaster Recovery Plan for the mainframe and mid-range environments to ensure currency of what is to be recovered and procedures governing the recovery.

13.2. The test and implementation aspects have to be kept current and in synchronisation with business changes. All changes to the business and in the mainframe and mid-range environments must be considered for inclusion in, and for updating of the Disaster Recovery Plan.

13.3. The Disaster Recovery Plan may require updates if problems or changes occur in any of the following areas:

13.3.1. Mid-Range Disaster Recovery Test results.

13.3.2. New critical applications or critical customers.

13.3.3. Increased application complexity.

13.3.4. New equipment acquisitions.

13.3.5. Changes to:

13.3.5.1. Hardware.

13.3.5.2. Software.

13.3.5.3. Network.

13.3.5.4. Applications.

13.3.5.5. Data.

13.4. A formal review of a Disaster Recovery Plan should be conducted annually.

13.5. A quarterly Disaster Recovery Readiness Assessment Audit should be conducted.

13.6. The purpose of the reviews and the audits is to identify any changes to ensure that these and any other updates identified since the previous review have been captured.

13.7. The Disaster Recovery Plan aspects to be reviewed include the following:

13.7.1. Personnel changes.

13.7.2. Mission changes.

13.7.3. Priority changes.

13.7.4. New Business Organisations.

13.7.5. Mid-range Disaster Recovery Test procedures and results.

13.7.6. Backup procedures.

13.7.7. Recovery procedures.

13.7.8. Relocation Migration Plan.

13.7.9. Software (operating system, utilities, application programs).

13.7.10. Hardware (mainframe, mid-range and peripherals).

13.7.11. Communications Network Facilities.

13.8. Particular attention should be paid to the review of the recovery equipment configurations to ensure that the business has the required equipment to restore the business functionality as quickly and smoothly as possible.

13.9. Recovery equipment reviews will require the time and attention of all Plan holders and team members, especially those that have hardware and network responsibilities.

13.10. The proper maintenance of the Disaster Recovery Plan will be the responsibility of all holders of the Plan. It will be the Plan holders' responsibility to incorporate all approved revisions into their assigned copy to ensure that the Plan manual is maintained as a viable and readied Action Plan.

13.11. All removed pages are to be properly disposed. It is the responsibility of all Plan holders to protect confidential material and dispose of it in a proper manner.

14. Disaster Recovery Testing Elements

14.1. The purpose of the Test Plan Document is to specifically identify and document the task plan and procedures to be implemented in a testing environment.

14.2. The Test Plan includes test parameters, objectives, measurement criteria, test methodology, task plan charts and timelines to validate the effectiveness of the current Disaster Recovery Plan.

14.3. The Disaster Recovery Plan will be tested to ensure that the business has the ability to continue the critical business processes in the event of a disaster, and that the recovery procedures are executable and accurate.

14.4. Testing of the plan includes training the personnel who will be responsible for executing the Disaster Recovery Plan.

14.5. Test results and problems encountered are to be reviewed and used to update or revise the current procedures.

14.6. Testing can be accomplished by executing the Test Plan or it may be desirable to execute a sub-set of the plan.

14.7. When performing a disaster recovery test, only information which is recalled from the off-site storage facility should be used.

14.8. The purpose is to:

14.8.1. Simulate the conditions of an actual crisis management situation.

14.8.2. Completeness of the disaster recovery information stored at the Records Retention Site.

14.8.3. Ensure the ability to recover the intended functions.

14.9. The test plan includes the following areas:

14.9.1. **Schedule**

14.9.1.1. Planning Sessions.

14.9.1.2. Pre-Test Technical Review.

14.9.1.3. Debriefing.

14.9.2. **Introduction**

14.9.2.1. Preface.
14.9.2.2. Scope.
14.9.2.3. Recovery Site.
14.9.2.4. Primary Test Objectives.
14.9.2.5. Secondary Test Objectives.
14.9.2.6. Exclusion (if applicable).
14.9.2.7. Test Assumptions, Dependences and Success Criteria.

14.9.3. **Test Teams**

14.9.3.1. Choice-Point Participants.

14.9.4. **Pre-Test Planning**

14.9.4.1. Activities.
14.9.4.2. Issues.
14.9.4.3. Concerns.

14.9.5. **Test Timeline**

14.9.5.1. Planned start and stop time of test and tasks.
14.9.5.2. Actual start and stop time of test and tasks (to be completed during the test).

14.9.6. **Critical Test Checkpoints**

14.9.6.1. Activity.

14.9.6.2. Recommendation.

14.9.6.3. Responsible party.

14.9.7. **Test Problem Log**

14.9.7.1. Document any problems encountered prior to the test.

14.9.7.2. Record any deviations from Test Plan.

15. Post Test Review

15.1. The purpose of the Post Test Review document is to identify any problem areas and any recommendations for improvement to the plan.

15.2. The Post Test Review document includes the following areas:

15.2.1. **Overview**

15.2.1.1. Overall Test Results.

15.2.1.2. Test Dates.

15.2.1.3. Disaster Recovery Back-up Site.

15.2.1.4. Local Access Suite.

15.2.1.5. Test Participants.

15.2.2. **Test Objectives**

15.2.2.1. Primary Test Objectives.

15.2.2.2. Secondary Test Objectives.

15.2.2.3. Exclusions (if applicable).

15.2.3. **Timeline**

15.2.3.1. Planned task, start and end times and duration.

15.2.3.2. Actual task, start and end times.

15.2.4. **Problems Encountered During the Test - Problem Log**

15.2.4.1. Actual Problem.

15.2.4.2. Assigned to.

15.2.4.3. Target Date for Resolution.

15.2.4.4. Status.

15.2.4.5. Resolution.

.

15.2.5. **Problem Summary**

15.2.5.1. Follow up to pre-test problems.

15.2.5.2. Follow up to suggestions for improvement/recommendations from previous year's test.

15.2.5.3. Detailed summary and observations.

15.2.5.4. Recommendations for the following year's test.

16. Roles And Responsibilities Disaster Recovery Continuity Culture

16.1. Implement the recommendations made across the entire business.

16.2. Provide a training programme for those directly involved in the execution of the Disaster Recovery Plan.

16.3. Provide an education and awareness session to ensure enterprise-wide understanding and adoption of the Disaster Recovery Plan, covering internal and external stakeholders; employees, customers, suppliers, shareholders and third parties upon whom the institution depends/have influence in both normal and crisis operations.

16.4. Select the Emergency Management, Business Communication and Crisis Recovery Teams.

16.5. Implement relevant training sessions for each team dependent upon task, including crisis communications/media training as appropriate.

16.6. Establish and equip emergency crisis centres with the necessary resources.

16.7. Establish internal and external contractual arrangements and service level agreements.

16.8. Implement back-up and off-site storage arrangements.

16.9. Distribute plan documentation as appropriate.

16.10. Conduct internal and external awareness sessions incorporated into employee and supplier induction processes and customer marketing programmes.

17. Disaster Recovery Education For Employees

17.1. Educate employees about where to store their files (in a specific directory on their computer that is backed up or on the central server) to ensure that all files are included in the backup.

17.2. Avoid data loss and downtime by installing anti-virus software and informing employees how viruses are spread.

17.3. Communicate typical processes and turnaround times that customers have come to expect.

17.4. Inform employees how to prioritise recovery efforts.

17.5. Ensure all employees know whom to contact in an emergency situation, and outline what they can do to remain productive during the recovery period.

17.6. If making use of external service, identify who in the company will contact the service provider to initiate recovery efforts. Ensure the contact information is available off-site in case of a fire, flood, or other act of nature.

18. Review Of This Policy

Regular review and amendment of this policy will be done in line with the approved institutional policies. This will take place in consultation with the relevant quality assurance structures at departmental and institutional level, under the auspices of the official custodian of this policy, namely the Executive: Operations.

19. Revision History

Version No.	Amendment Details	Approval date	Approving Committee	Chairperson Signature
Version 1 (V1)	Various	16/08/2019	A/BOARD	
Version 2 (V2)	Amendments as per review tracking document: Amendment review	11/04/204	The Board	