GOVERNMENT OF NEPAL
MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY

Disaster Recovery Plan Template

< Project Name>

Date

Version 1.0

Authors

[Client details],		

Version history

		Draft		Final	
Description	*Version*	*Draft Date*	*Author*	*Approval Date*	*Approver*

Table of contents

<ITALICS are special instructions for completing the template. When creating a template, insert detailed instructions in italics. Before finalising a deliverable, ***DELETE all italic text****, instructions and unused material.*

- *On Title Page: Insert document name and date of submission;*
- *On Author and Version History Page:*
  - *Author Table: Insert author names and delete generic references;*
  - *Version History Table: track ongoing history of changes to this document. Approver should be highest level person, persons or committee required to validate and adopt this document;*
  - *Copyright Version: May require adjustment based on the Terms and Conditions of the Engagement Contract. Year reference may require adjustment based on current date;*
  - *Select View>>Header and Footer to adjust Headers/Footers. Select item, right click and select Update Field.*
- *On the Table of Contents Page: Right Click within the Table of Contents. Select Update Field>>Update Entire Table;*
- *This document contains generic text and formatting references to assist in development. Adjust, duplicate by adding additional sections, build on and replace this text as appropriate for your document;*
- *When using this template to create a Technique, the following applies:*
  - *Reference the Activity(ies) or Deliverable(s) the Technique applies to;*
  - *Describe parameters of use (for example, only applies to federal agencies, only applies to specific technology);*
  - *Describe the advantages of following the technique's leading practice (for example, time savings, skills required, quality).*

1. Introduction

<Provide an introduction to the Disaster Recovery Plan deliverable and the process utilised to gather the appropriate information to support the creation of this deliverable. Sample text and recommended content sections are provided below. Edit, add and revise as needed to fulfil the requirements of the client.

This deliverable may be added to and/or revised through several activities during the course of the project. At the outset of the project, you may only work on certain sections for a given activity. When efforts within the Assess stage, review and profiling of the IT Disaster Recovery Plan (DRP) and environment will tend to be at a high-level, consistent with that necessary to make strategic decisions about the DRP Strategy. Inventory and analysis efforts typically take place during the Design, building on the initial profile developed during the Assess stage. Please consult the Engagement Manager to find out which sections of this deliverable are required for the current activity, and which ones can be postponed until a later activity.>

The purpose of this deliverable is to provide a high-level description of the Disaster Recovery Plan and strategy for application(s) and/or infrastructure relevant to this project. The Disaster Recovery Plan design also includes the physical and logical strategies for continuity and recovery of the data centre, server platforms, network devices, database, applications, and data. The designated project team member(s) will need to conduct client reviews of the current state disaster recovery plan findings and validate disaster recovery plan design strategies appropriate for the project.

1.1. Approach

<Describe the approach used to complete this deliverable. Sample text and recommended content sections are provided below. Edit, add and revise as needed to fulfil the requirements of the client.>

The following process will be used to capture the necessary information:

Document the infrastructure disaster recovery plan at the *<Client Name Here>* locations supporting the *<Program Name Here>* implementation and the *<Project Name Here>* application *<in the event that the project is driven by a major application implementation initiative.>*. The focus shall be on the review and analysis of the *<Client Name Here>* current state disaster recovery plans of business units, their technical resources, and from the *<Project Name Here>* team members.

Review the defined infrastructure disaster recovery constraints and dependencies imposed within the internal and external organisation (e.g. business impact analysis, business issues, such as budget constraints, vendor contracts, and active/planned projects; management issues, such as leverage of existing assets and internal political concerns/boundaries; physical constraints, such as proximity to vendor/carrier sites and data centre space limitations).

Develop an understanding of the client's short and long-term vision of the enterprise's technical infrastructure and applications within the evolving business environment.

The scope of this document will be to build upon the policy, procedural, and reference documents already in place at *<Client Name Here>* for the *<Project Name Here>* team for those areas and activities affected by this project. This Infrastructure Disaster Recovery Plan design document is not intended to replace current documentation. Instead, it represents a summarisation and analysis of the documents already in place, and will additionally contain information that needs to be created from existing information that may come from discussions with <Project Name Here> team members. By reviewing findings with the affected business units and Information Technology (IT) resources associated with the client's current state infrastructure disaster recovery planning and strategy, these reviews shall form the basis for conducting a limited or enterprise–wide Business Impact Analysis (BIA) to leverage the current technology (where appropriate) and build upon the existing disaster recovery plans or leverage economies of scale for common disaster recovery business unit needs to reduce the cost of the overall program. Reference BIA information and templates provided by the Assess Operational Environment activity of the Production Services work stream. Store the identified documentation and any other supporting documentation in Appendix A.

2. *disaster recovery plan design areas*

<This section highlights the organisational aspects and infrastructure disaster recovery and continuity areas that can be the focus of this review process, depending upon the specific needs of the project team. While different methods can be used to organise the data collected, it is important to characterise the data in a way that helps highlight the overall value that the existing disaster recovery plan and strategies have in supporting the current and future business, and identifying those strategies that will be carried forward in their current form, migrated, upgraded or retired.

Additionally, the baseline activities may collect and organise information about dependencies, vendor support, outsourcing, or other issues critical to the business processes and their use of current disaster recovery strategies. Use the following as a guide to organising and executing the tasks required to complete this deliverable.

The following sections may also be used to organise and capture the information about the enterprise's disaster recovery plan design. Compile this information into the format that is most useful for this project.

- ***Business Impact Analysis*** *– Refers to the service performed internally or externally to understand and document the impact of a sustained business process outage. Based on that, define the business continuity/disaster recovery requirements in terms of resources required and recovery needs, and recovery capabilities. The business impact analysis can be performed to include all business processes or just the specific business unit focus of a project. Reference the [Client] Delivery Framework Production Services work stream's Assess Operational Environment activity. From this activity, a current Business Impact Analysis may be available;*
- ***Infrastructure/Platform Recovery Time Objectives (RTOs)*** *– Refers to the identification and documentation of the recovery time objectives of the critical business processes relevant to the project. Documentation of the Information Technology organisation's capability or internal service level agreements (SLAs) to meet those recovery time objectives for recovering the relevant infrastructure components after a disruption or disaster event. This information is typically compiled and available in a Business Impact Analysis;*
- ***Business Continuity Plan Policy*** *– Refers to the Policy outlining daily operational procedures and practices characteristics of the Corporate Business Continuity Program policies that are written to ensure continuity and recovery for network, application, and facilities infrastructure components. These BCP plans and policies also limit organisational exposures;*
- ***Continuity & Recovery Procedures for Network Connectivity*** *– Refers to disaster*
- *recovery plan processes & procedures for continuity & recovery of the LAN/WAN network infrastructure components;*
- ***Telephony Continuity & Recovery Procedures*** *– Refers to disaster recovery plan processes & procedures for continuity & recovery of the Telephony infrastructure components;*
- ***Equipment Replacement Procedures*** *– Refers to the equipment replacement procedures for disaster recovery plans in the event critical equipment is damaged or destroyed during a disaster event. This plan should reference SLAs with relevant vendors to provide and deliver the described equipment to specific locations within an outlined timeframe to meet recovery time objectives;*
- ***Tape Backup & Retrieval Procedures*** *– Refers to characteristics of tape backup procedures, backup type, frequency, equipment, off site storage, Vendor, retrieval process and SLAs;*
- ***Platforms & Operating Systems Recovery Procedures*** *– Refers to disaster recovery plan processes & procedures for continuity & recovery of the Platform & Operating Systems infrastructure components;*
- ***Continuity & Recovery Procedures for Databases*** *– Refers to disaster recovery plan processes & procedures for continuity & recovery of the Databases for platform components;*
- ***Continuity & Recovery Procedures for Packaged Applications*** *– Refers to disaster recovery plan processes & procedures for continuity & recovery of the Packaged Applications (e.g. SAP, ERP) infrastructure components;*

- ***Primary/Alternate Facilities & Recovery Sites*** *– Refers to the physical disaster recovery characteristics of the primary facility, computer rooms and wiring closets, along with the alternate site and or recovery facilities;*
- ***Emergency Response/Crisis Management (ER/CM) plans*** *– Refers to emergency response and crisis management team structure, processes & procedures that address the many elements of effectively responding to a crisis. These include: Responding to life/health/safety issues, Damage mitigation (containment), Damage assessment (measurement), Disaster declaration criteria and protocols, Crisis Communications Modelling (CCM), Coordination with first responders, and transition from crisis response to disaster recovery.>.*

The collection of data about the enterprise and its information technology (IT) disaster recovery plan should cover as many perspectives and dimensions relative to this project as possible. Detailed information need not be compiled, but should be available if necessary to understand the assumptions embodied in the summary.

3. design processes

<The following sections describe activities that are performed, the key types of work products produced, and resources that can be used to support these activities.>

This...

3.1. Design analysis activities

<Utilise the Current State Infrastructure Disaster Recovery Plan document findings that were analysed to determine how well the existing business processes, infrastructure components, and disaster recovery plans work together. The designated project team member(s) will need to conduct client reviews of the current state disaster recovery plan findings and validate disaster recovery plan design strategies appropriate for the project. These review activities will be used for further determining those parts that are worth building on, and those parts that should be retired. This analysis may take the form of sets of matrices and general heuristics, such as using values of low/high or useful/not useful. The focus of the analysis is to get the most pressing concerns analysed with recommendations for improvements to ensure that the disaster recovery plans address the areas needing to be improved. Not every system identified will be improved, and not every system will be improved at the same time.

The typical areas of analysis are:

- *Utilise the Current State Disaster Recovery Plan Review Findings to document alternative strategies and improvements that would be reflected in the Disaster Recovery Plan Design;*
- *Work (Business): Critical business processes and functions, the work that is performed, the disaster recovery plans that support the critical business processes) as defined in previous section;*
- *Disaster Recovery Plans for infrastructure components: (Email, Platforms, Network, Emergency Response & Management Plan.) As defined in previous section;*
- *Strengths and weaknesses of infrastructure disaster recovery plan strategy; level of standardisation; technology obsolescence; quality of infrastructure components; infrastructure disaster recovery services provided and service levels, cost breakdowns.*

The specific analysis process may be augmented and specialised with items specific to the scope of the project. This may include those things particular to the enterprise's business and its technological environment (e.g. centralised, distributed, global-international). The analysis team should strive to keep their terminology consistent across the enterprise. A list of references of all data sources, such as disaster recovery plans, configuration management reports, inventory lists, interviews, email, and other sources, should be maintained. This will help to assess any uncertainty in the accuracy of the characterisation and help others to tap these sources again if necessary.>

This...

4. Disaster recovery plan design

<This section would typically be included as part of other activities in the Design stage, as it will document infrastructure disaster recovery plans component details that comprise the client's production and non-production technical infrastructure environment. Based on the high-level information gathered to document the Current State Disaster Recovery Plan, this section may be used to drill down into components/elements of the client's disaster recovery plan strategy. Document strategic alternatives and design considerations that support improved Disaster Recovery within the client's environment, and specify if appropriate the physical and logical aspects of corporate standards. Considerations should support simplicity within the client's environment, and how disaster recovery, management, maintenance and user interfacing complies with recovery time objectives or internal service level agreements. Some areas that could be addressed are included below.>

This...

4.1. Infrastructure/Platform recovery time objectives (RTOs)

<Document the recovery time objective considerations and recommendations for the critical business processes relevant to the project. Documentation of any known limitations based on the Information Technology organisation's capability or internal service level agreements (SLAs) in place to meet those recovery time objectives for recovery of those infrastructure components relative to the project after a disruption or disaster event.>

This...

***Table 2-Infrastructure/Platform Recovery Time Objectives (RTOs)**

No.	Infrastructure Component/RTO	IT Organization RTO Capability	Limitations/Comments
1			
2			
3			

4.2. Business continuity plan policy

<Document disaster recovery plan compliance considerations, enhancements, and recommendations that support best practices within the client's environment relative to this project, and if applicable, to support the enterprise's business continuity plan (BCP) or continuity of operations (COOP) Standards. For example, NIST, ISO17799, BS7799, NSA. Reference Transform A1.1 Review and articulate the business strategy. For situations in which ongoing operations and BCP management are expected, the practitioner should refer to Business Continuity Plan planning, documentation and operations. >

This...

4.3. Disaster recovery vulnerability/threats

<Document identified vulnerabilities and design considerations that will reasonably address identified threats or vulnerabilities. For example, Single Points of Failure.>

This...

***Table 3-Disaster Recovery Vulnerability/Threats**

No.	Vulnerability	Design Considerations for Improvements
1		
2		
3		

4.4. Continuity and recovery procedures for network connectivity

<Document current state network LAN/WAN disaster recovery strategy and limitations. Then document high level strategic alternatives and design considerations relative to this project that support network continuity and recovery improvements within the client's environment. The current strategy and known limitations are based on current technology and infrastructure architecture.>

This...

***Table 4-Continuity & Recovery Procedures for Network Connectivity**

No.	Current Recovery Procedure/Strategy	Design/Strategic Alternative for Improvement
1		
2		
3		

4.5. Telephony continuity and recovery procedures

<Document design considerations that will address telephony disaster recovery plan improvements with the client's environment, and any known limitations based on current technology and infrastructure architecture relative to this project.>

This...

4.6. Equipment replacement procedures

<Document the strategy and limitations of current equipment replacement procedures for disaster recovery plans in the event critical equipment is damaged or destroyed during a disaster event. This plan should reference service level agreements (SLAs) with relevant vendors to provide and deliver the described equipment to specific locations within an outlined timeframe to meet recovery time objectives. Document high level strategy and or vendor negotiations that will address equipment replacement needs improvements for disaster recovery plans within the client's environment, and any known limitations based on current technology and infrastructure architecture relative to this project.>

This...

4.7. Platforms and operating systems recovery procedures

<Document current Platform and Operating System recovery procedures strategy and limitations. Then document high level strategic alternatives and design considerations that will address Platforms and Operating Systems disaster recovery improvements within the client's environment, and any other known limitations based on the current technology and current infrastructure disaster recovery plans relative to this project.>

This...

4.8. Continuity and recovery procedures for applications/data

<Document current applications/data recovery strategies and limitations. Then document high-level strategic alternatives and design considerations that will address application/data disaster recovery improvements within the client's environment, and any other known limitations or dependencies based on current technology and infrastructure architecture relative to this project. For example, Application, Packaged Applications, Applications Data.>

This...

4.9. Primary/alternate facilities for recovery

<Document current Facilities disaster recovery strategies and limitations relative to this project. Document high-level strategic alternatives and design considerations that support disaster recovery improvements for buildings, computer rooms, access systems and disaster recovery plan strategies used in the facilities relative to this project within the client's environment, and any other known limitations based on current technology and facilities infrastructure architecture. If applicable, document disaster recovery service provider facility service levels. Is a formal data centre capacity planning and design services engagement required?>

This...

5. Disaster recovery plan assumptions

<In this section, provide a listing of any assumptions the project team has used in providing the above baseline information. This can be offered in text format, or provided in a table pulled from a spreadsheet. Some sample assumptions could include:

- *Business impact analysis has not been performed for this business process;*
- *A formal engagement for the identification of strategic alternatives for continuity and recovery will be proposed and performed. The completion of the Disaster Recovery Plan will be performed after implementation of strategic alternatives;*
- *Technology refresh process has been outsourced, and contract review was not in-scope;*
- *Legacy application consolidation project is currently in progress;*
- *Currently there is no disaster recovery plan in place for the infrastructure technology relative to the project;*
- *Currently there is no business continuity plan or policy in place>.*

This…

<The following section contains possible additional paragraphs you may wish to include in your document. Use any or all of these paragraphs, or if none, then delete the entire section.

Any of the information below may be provided in a list in the body of this document, as a reference to an appendix, or as a reference to another document.>

6. Additional information

6.1. Acronyms, abbreviations and definitions

<Provide an alphabetical listing of acronyms, abbreviations, terms and definitions needed to understand this document.>

6.2. Open issues and future considerations

<If there are known issues, risks or considerations: describe, give timeframe, possible resolution>

6.3. References and related documents

<List the title, version/publishing date of referenced documents, websites, or other relevant references. If copyrighted documents are referred to, the copyright information must be appropriately referenced.>

7. Appendices

<Appendices may be used to provide information published separately for convenient document maintenance, such as classified data, or for providing supplemental material. The main body of the document should contain at least one reference to each Appendix. Appendices are listed in alphabetical progression (A,B,C).>

7.1. Appendix A – Detailed supporting documentation

This...

7.1.1. Recent business impact analysis

This...

7.1.2. Current disaster recovery plans

This...

7.1.3. Disaster recovery/business continuity test history

This...

7.1.4. Emergency response and crisis communications plans

This...

7.2. Appendix B – Title