**<< Application Number - Application Name >>**

**Disaster Recovery**

**Template**

**Disaster Recovery Checklist**

**Purpose**

The Disaster Recovery Checklist is an outline of the detailed steps required to restore the infrastructure and application in the event of a disaster.

Important Notes for Completing this Document

* This template must be used by all teams in the creation of Disaster Recovery plans. A Disaster Recovery Analyst will be assigned to assist in the completion of the document. Please contact OCIODisasterRecovery@gov.nl.ca for assistance.
* All sections of this document are to be completed unless otherwise noted.
* Insert the TRIM document number into the footer. Project teams can obtain a document number from the ISC (ocioisc@gov.nl.ca).
* Text contained within << >> provides information on how to complete that section and should be deleted once the section has been completed.
* This Checklist Template How To page can also be deleted from the final document (before signatures).
* Please color ALL net new text blue to differentiate it from the rest of the document.
* Once the Checklist has been completed, (before signatures) remove the word “Template” from the cover page.
* The final version of this Checklist must be approved by those noted on the DR Checklist Approvals page. This approval may be granted by email.

**Table of Contents**

[System Overview 4](#_Toc262128416)

[Checklist Maintenance Procedures 5](#_Toc262128417)

[Applications Included in This Checklist 6](#_Toc262128418)

[Introduction to Recovering the IT or IM System or Service 7](#_Toc262128419)

[Part 1 - Use of Hot Site Resources 8](#_Toc262128420)

[Part 2 - Application Restoration 9](#_Toc262128421)

[Part 3 – Reconfigure and Reconnect 10](#_Toc262128422)

[Part 4 – Operational Testing 11](#_Toc262128423)

[Annex A – DR Checklist Change Log Sheet 12](#_Toc262128424)

[Annex B – Data Cleanup 13](#_Toc262128425)

[Annex C – DR Checklist Approvals 14](#_Toc262128426)

| System Overview |
| --- |
| **Application Description** | << Provide a brief description of the application >> |
| **Platform** | << Provide application platform details >> |
| **Technology** | << Provide an overview of the technology used to build the application >> |
| **Recovery Strategy** | << Provide suggested recovery strategy details >> |
| **Assumptions** | << Provide assumptions to the successful recovery of the application >> |

|  |  |
| --- | --- |
| Checklist Name | << Application Number – Application Name >> |
| Checklist Owner | Name: << Insert Name >>Title: << Manager, Application Services or Manager, Operations >>Work Number: << Insert Work Number >>Cell Number: << Insert Cell Number >>Home Phone Number: << Insert Home Number >>E-Mail: << Insert E-Mail Address >> |
| Checklist Author | Name: << Insert Name of Project Team Member >>Title: << Insert Title >> Work Number: << Insert Work Number >>Cell Number: << Insert Cell Number >>E-Mail: << Insert E-Mail Address >> |
| Checklist Maintained By | Name: << Insert Name >>Title: << Manager, Application Services or Manager, Operations >>Work Number: << Insert Work Number >>Cell Number: << Insert Cell Number >>Home Phone Number: << Insert Home Number >>E-Mail: << Insert E-Mail Address >> |

## Checklist Maintenance Procedures

The procedures for maintaining this Checklist are:

* **Review Cycle** – The DR Analysts will coordinate periodic reviews with the DR Checklist owner to ensure the accuracy of the DR Checklist content.
* **Review after Configuration Change** – This Checklist will be reviewed and updated as required when there is any change to a system, application, hardware, network connection or security mechanism configuration of the system or application or service for which this Checklist is developed.
* **Making Suggestions For Changes To The Checklist** – All OCIO staff are encouraged to provide suggestions and recommendations to the OCIO DR Specialist Team Leader, appropriate Director or appropriate Branch Executive Director for consideration
* **Checklist Approval Process** – This Checklist must be approved by those listed in Annex C, DR Checklist Approvals. Once approved, the updated Checklist will be forwarded to the ISC.

**General Checklist Assumptions:** The assumptions used in developing this Checklist are:

* **Government DR Site** – The Government DR Site is in place, provisioned with necessary equipment and is accessible.

## Applications Included in This Checklist

| Application Number | Application Name | Department |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Introduction to Recovering the IT or IM System or Service

**Recovery Procedures and Checklists**

Once directed to do so and once on site, the OCIO DR Specialist Team will begin to recover the disrupted or damaged IT or IM system or service following:

* The procedures detailed in Part 6 of the DR Management Framework;
* Any additional instructions provided by the OCIO Emergency Operations Center (EOC);
* The instructions and information contained in the Team Manuals; and,
* The recovery process contained in this Checklist.

DO NOT TALK TO THE NEWS MEDIA
REFER MEDIA TO THE COMMUNICATIONS/PUBLIC AFFAIRS BRANCH

## Part 1 - Use of Hot Site Resources

**(IF APPLICABLE)**

If a hot site backup or fail over capability for the IT or IM system or service is available, the Team Leader will ensure that the IT or IM system or service has failed over correctly to the hot site and is operating correctly from the hot site back up using the backup configuration.

| **#** | **Item** | **Details** |
| --- | --- | --- |
| **1** | Description of Backup / Fail Over Capability |  |
| **2** | Description of how that backup / fail over capability is activated |  |
| **3** | How to Determine that the backup / fail over capability has worked properly |  |
| **4** | Once the failed system has been recovered, how the system will be returned to the main site from the backup / fail over site |  |

## Part 2 - Application Restoration

**(Complete for Application Server, Application, Database Server and Database as applicable)**

The Team will recover the system, application or service as follows:

| **#** | **Description** | **Specific tasks** |
| --- | --- | --- |
| **1** | Repair / rebuild or replace damaged / non-functioning hardware, firmware and software:* Use spare / replacement resources in the work place or in the recovery box
* If no spare / replacement resources are available, the Team Leader will order replacement items from suppliers
 | **Application Server Recovery***Consider:**System Requirements**Hardware Requirements**Software installation**Refer to Build Books as Applicable***Database Server Recovery***Consider:**System Requirements**Hardware Requirements**Server Configuration Notes**TSM Configuration**Files to Restore**Current Networking Configuration**Routing Table**Configuring SSH**Refer to Build Books as Applicable* |
| **2** | Reload all required software and data | **Application Recovery***Refer to Build Books/ OPM as Applicable***Database Recovery***Consider:**Oracle software installation**Database Restore**Refer to Build Books/ OPM as Applicable**Note Location of Back-ups* |

## Part 3 – Reconfigure and Reconnect

Once the system, application or service has been repaired, tested and is working properly, the system, application or service will next be reconnected to the network.

| **#** | **STEP** | **SPECIFIC TASKS** |
| --- | --- | --- |
| **1** | Verify network connectivity – check all network connections (gateways, routers, switches, cabling) and addressing |  |
| **2** | Verify security mechanisms, settings and configuration (firewalls, access control mechanisms) |  |
| **3** | Connect IT or IM system or service to the network |  |
| **4** | Perform operational test over the network to ensure that IT or IM system, application or service works correctly over the network |  |

## Part 4 – Operational Testing

Once the system, application or service has been reconnected to the network, the Team will perform the following operational tests to confirm that the system, application or service is operating correctly.

| **#** | **STEP** | **SPECIFIC TASKS** |
| --- | --- | --- |
| **1** | Test the IT or IM system, application or service to ensure proper operation |  |
| **2** | Test all network connections |  |
| **3** | Test all interdependencies with other systems, applications and services to ensure that interdependencies work correctly |  |
| **4** | Test the security configuration, mechanisms and settings from end user perspective |  |
| **5** | Test an end user connection over the network to test the recovered system, application or service. |  |

# Annex A – DR Checklist Change Log Sheet

**Notes:** All dates will be shown as YYYY-MM-DD. A change entry will be made to show the name of the person responsible for making the update as well as the manager(s) responsible for approving the change.

| **#** | **Date** | **Section Updated** | **Update Reason** | **Change Initiator Signature** | **AS Manager Signature** | **DR Manager Signature** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Annex B – Data Cleanup

Following a DR Scenario the data on all DR Servers must be completely removed.

<< Example below is for removing a VM, if this does not apply please delete and provide specific details >>

**VMware Servers:**

* Disaster Recovery Analyst(s) to confirm successful DR scenario with client
* Disaster Recovery Analyst(s) to confirm the list of Virtual Machines (servers) used in the scenario that are now ready for decommission and deletion
	+ Note that some VM(s) may host services which other “live” scenarios continue to depend upon & may not be candidates for deletion
* Disaster Recovery Analyst(s) to submit an OVSD Work Order to Enterprise Services referencing the specific VM(s) to delete
	+ Note that unneeded vLANS associated with the servers could also be removed at this time due to vLAN constraints
	+ Individual client access that is no longer needed could be removed at this time in an effort to avoid “access issues” in the future
* Enterprise Services Team to execute tasks as defined in the Work Order & send successful confirmation to the Disaster Recovery Analyst(s)
	+ Detailed task list by function is defined below:

**Decommission & Deletion of a Virtual Machine(s):**

* Once these steps are executed, the selected Virtual Machine is destroyed and not recoverable…
	+ From within the Virtual Infrastructure Client, select the targeted VM
	+ Power off the VM
	+ Right-click on the VM within the inventory
	+ Select Delete from Disk

**Removing vLAN(s)**

* This must be completed an ALL ESX host servers within the cluster
	+ From within the Virtual Infrastructure Client, highlight the host ESX server
	+ Select the configuration tab from the summary screen
	+ Select networking from the hardware section of the configuration screen
	+ Find the correct virtual switch that the VLAN is attached to
	+ Select properties
	+ On the virtual switch properties screen highlight the vLAN number
	+ Press remove

**Removing Client(s) Access:**

* Client access is revoked by removing the users PSNL account from the local access group on the Virtual Center server
	+ Initiate a RDP session to the Virtual Center Server (10.50.201.51)
	+ Log into the server using PSNL administrative credentials
	+ Open the Computer Management \ Local Users and Groups \ Groups applet
	+ Open the group VMware\_Disaster\_Recovery\_Test\_Site\_Users
	+ Highlight the user to be removed
	+ Press remove

## Annex C – DR Checklist Approvals

| Submitted by | Signature | Date |
| --- | --- | --- |
| Project Manager: |  |  |

***The above signature confirms that suitable Build Books and OPMs are in place.***

| Approval Role | Signature | Date |
| --- | --- | --- |
| Solution Delivery Manager: |  |  |
| Application Services Manager: |  |  |
| Operations Manager: |  |  |
| DR Manager: |  |  |