|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **System Name:** |  |  | **Version:** | 1.0 |
| **Created By:** |  |  | **Created Date:** | 2013-03-01 |
| **Last Updated By:** |  |  | **Last Updated Date:** | 2013-06-26 |

**Overview of Disaster Recovery (DR) Process:**

|  |
| --- |
| <Description of the DR process at a high-level. This should give context to the rest of the document.> |

**Definition of Disaster:**

|  |
| --- |
| <Loss of a certain degree of functionality, loss of certain modules, etc… A scenario that fulfills this definition will kick off the formal DR process.> |

**Coordination with Infrastructure Disaster Recovery:**

|  |
| --- |
| <How does the system disaster recovery process interact with possibly simultaneous DR from the TSC? What network and infrastructure components are required before any system DR can happen?> |

**Disaster Recovery Team:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | DR Role | DR Responsibilities | Phone (Work + Home) | Email |
| <John Doe> | DR Lead | <Makes DR decisions. First to be contacted. Initiates disaster recovery process. Contacts other.> | 1-867- 1-867- | @gov.nt.ca @gmail.com |
| <Jane Doe> | DR Team | <Other members of the DR team> |  |  |
| <John Doe> | TSC Liaison | <Single point of contact at TSC for duration of disaster.> |  |  |
| <Other roles> |  | <Consider communications, finance, other departments, business team members, etc…> |  |  |

**Help Using This Template**

The Disaster Recovery Plan describes the process of recovering the system from a disaster. It also provides information that would be critical in such a scenario. This plan is particular to a single system and thus, it should be developed as part of a larger departmental DRP, as well as a corporate infrastructure DRP (owned by the TSC). These broader plans are critical for prioritizing systems for recovery. However, this plan is also critical, and should be constantly on-hand and reviewed periodically. For help completing the DRP or for relevant examples, contact the [Corporate Information Security Group of the OCIO](mailto:http://our.gnwt.ca/dept/fin/ocio/infosec/default.aspx).

*Delete this box after reading.*

**Communications Activities during a Disaster:**

|  |  |  |  |
| --- | --- | --- | --- |
| Audience | Format | Message | Timing |
| Minister | <Phone, email, mail, briefing note> | <The general content of the message> | <At which point in the DR process should the communication occur?> |
| Deputy Minister |  |  |  |
| Senior Managers |  |  |  |
| Program Managers |  |  |  |
| Users |  |  |  |
| Press |  |  |  |
| <Others audiences> |  |  |  |

**Data in Order of Criticality:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rank | Data | Data Type | Storage Type and Location | Back-up Frequency |
| 1 | <Data Name or Group> | <Confidential, Public, Personally identifying information> | <Database Type, Server Info, etc…> | <Frequency that data is backed up> |
| 2 |  |  |  |  |
| 3 |  |  |  |  |

**Components in Order to Be Restored:**

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Component Name | Type | Method of Recovery |
| 1 | <Component name> | <Application, middleware, module, etc…> | 1. <Reinstall steps, back-up recovery steps, patching steps, etc…> |
| 2 |  |  |  |
| 3 |  |  |  |

**DRP Testing Activities:**

|  |  |  |  |
| --- | --- | --- | --- |
| Activity | Description | Person Responsible | Frequency |
| DRP Review & Update | <This document is reviewed by the DR team and updated> | <Who will lead it or ensure it is done?> | <Yearly> |
| Walkthrough | <Team members verbally walk through the steps of a disaster recovery scenario> |  | <Yearly> |
| Simulation | <Disaster is simulated without any actual system failure> |  | <Yearly> |
| Parallel Test | <A real system outage is simulated on a parallel system> |  | <After major updates> |
| Full-Interruption Test | <A real system outage is simulated on the production system> |  | <Before go-live> |
| <Other Tests> |  |  |  |