


Policy Title:	Disaster Recovery Plan Policy		
	INFORMATION TECHNOLOGY SERVICES (ITS)	Category	Information Technology Services
		Administrative Policy #	
		Revision #	
		Review Frequency	As Needed – no less frequently than triennially
Administrative Division	Information Technology Services (ITS)	Reviewed By	Chief Information Officer
BOWC Approval		Last Reviewed/Update Date	
Implementation Date			

1. OBJECTIVES

- 1.1. The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations.
- 1.2. An additional objective is to ensure that contingency arrangements are cost-effective.

2. PURPOSE

- 2.1. This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by DWSD. The disaster recovery plan ensures the recovery of critical ITS functions, systems and services when a disruption to operations occurs after a disaster or emergency situation.

3. DEFINITIONS

“Disaster” means an event that disrupts the normal function of a system or service.

“Disaster Recovery Plan” (DRP) means a technical document describing how an organization restores critical technology and business systems following an outage or disaster

"DMT" means Disaster Management Team – A team consisting of various individuals or departments who shall deal with the disaster and ensure to provide appropriate support during and after a disaster.

"Plan" means the strategic steps or tasks of execution.

4. SCOPE

- 4.1. This policy is directed to the ITS staff who are accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

5. RESPONSIBILITIES

5.1. Chief Information Officer (CIO)

- 5.1.1. The Chief Information Officer (CIO) is responsible for publishing this policy; communicating this policy to all employees; for review, approval and publishing of divisional standards; and updating this policy as necessary.
- 5.1.2. The CIO, or delegate, is responsible for interpreting and enforcing this policy.
- 5.1.3. The Department Director is responsible for declaring an actual emergency or state of Disaster Recovery.

6. POLICY

6.1. Risk Assessment

- 6.1.1. Loss of the infrastructure and ITS-managed systems and servers is a critical disruption to operations but the loss of data on any ITS-managed systems is an unacceptable risk. ITS has taken a multi-prong approach to minimize this risk and ensure that the infrastructure, systems and data can be restored in the most expeditious manner. The approach includes the following:
 - 6.1.1.1. DWSD is a cloud first organization.
 - 6.1.1.2. DWSD's enforces security and disaster recovery standards on selected service providers.
 - 6.1.1.3. DWSD imposes insurance limits and coverages on selected service providers that insure we have a financial recovery path, should one be needed.

6.2. Disaster Recovery Planning

- 6.2.1. ITS will develop, maintain and test an Organizational Wide Disaster Recovery Plan.
- 6.2.2. The plan will include a communications listing consisting of the names and positions of key personnel as well as contact information (phone number, alternate phone number, and email).
- 6.2.3. The plan will have a notification calling tree consisting of key personnel.
- 6.2.4. The Chief Information Officer will ensure that the Organization Wide Disaster Recovery Plan is reviewed and updated on an annual basis.
- 6.2.5. ITS will perform testing of the Organizational Wide Disaster Recovery Plan on an annual basis.

6.3. Levels of Disasters and Emergencies

6.3.1. Minor State

- 6.3.1.1. Minor incidents occur more frequently and the effects are often isolated to a small subset of critical business processes or areas. Business units that depend on these processes can continue to function for a certain duration of time and the cause is usually the failure of a single component, system or service.
- 6.3.1.2. Examples include the temporary loss of voice communications; network connectivity; data center servers; portal access; access to cloud-based services;

and the Service Desk incident management system, switchboard or telephone service.

6.3.2. Intermediate State

6.3.2.1. Intermediate incidents occur less frequently but with greater impact than minor incidents. These incidents impact portions of the building, disrupt normal operations of some but not all critical business units and generally result from major failures of multiple systems and equipment. ITS would activate a subset of the ITS disaster recovery plans.

6.3.2.2. Examples include malfunction of building administrative systems, water intrusion or leakage that displaces or disrupts data center systems and servers, loss of building communications closets or electrical disruptions that require generated power for longer than 4 hours.

6.3.3. Major State

6.3.3.1. Major incidents have a low possibility of occurring, but the extent has significant impact. These incidents disrupt normal operation of all critical business processes and involve the inaccessibility or failure of most systems and equipment. ITS would immediately enact an emergency state and activate the ITS disaster recovery plans.

6.3.3.2. Examples include fires, floods, earthquakes and sabotage.