Business Continuity and Disaster Recovery Policy

1.0 <u>Purpose</u>

The Office of Information Technology (OIT), like any other Maine State Government entity, is exposed to potential risks that could disrupt or destroy critical business functions and/or service delivery. OIT has developed this policy in support of a comprehensive program for OIT *Business Continuity*, *Disaster Recovery*, and overall business survivability.

Maine State Government and its citizens expect that critical government services will continue to function in the event of a disruption or major disaster. This policy outlines OIT's strategy to plan and respond to a major crisis in order to ensure OIT functions and services continue to operate as near to normal performance as possible while ensuring the safety and security of OIT employees.

2.0 <u>Definitions</u>

2.1 Business Continuity (BC): Ongoing process to ensure that necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.

2.2 Business Continuity / Disaster Recovery Manager: Coordinates planning and implementation for the overall recovery of the organization or business units.

2.3 Business Continuity / Disaster Recovery Planning Team: Responsible (in coordination with the BC/DR Manager) for planning, developing, and implementing business continuity related plans and projects. See Appendix B.

2.4 Business Continuity / Disaster Recovery Steering Committee: Provides direction, advice, guidance, and financial approval for BC/DR programs. See Appendix A.

2.5 Business Unit: A group of individuals organized to perform specific duties based on the functions performed within the organization. Examples of business units are: Finance, Operations, Applications Development, Client Technologies, Network Data Services, etc.

2.6 Crisis Management Team (CMT): Senior managers from each functional area (usually the BC/DR Steering Committee members) responsible for developing and implementing a comprehensive plan for responding to a disaster.

2.7 Disaster Recovery (DR): The technical aspect of Business Continuity. The collection of resources and activities to re-establish IT services (including components such as infrastructure, telecommunications, systems, applications and data) at an alternate site following a disruption. Disaster recovery includes subsequent resumption and restoration

of operations at a more permanent site. NOTE: DR does NOT have to occur at an alternate site if the current location is still suitable for DR procedures, but this is not typical.

2.8 Disaster Recovery Team(s) (DRT): A team (or teams) directed by the CMT to respond to a disaster. Can be comprised of multifunctional team members or divided into multiple specialty teams depending on the scope of the disaster. Led by the DRT leader (as appointed by the CMT).

2.9 OIT Emergency Operations Center: Default command and control location (51 Commerce Drive, Room 412).

3.0 <u>Applicability</u>

This policy ONLY applies to OIT, all of its functional areas, and employees. It does not apply to agencies external to OIT, even though they may consume services provided by OIT.

4.0 <u>Responsibilities</u>

4.1 This policy is enforced by the Business Continuity & Disaster Recovery Manager, OIT

4.2 Planning, Testing, and Program Maintenance

 4.2.1 *Business Continuity / Disaster Recovery (BC/DR) Steering Committee*:
  4.2.1.1 Provides guidance and oversight for the BC/DR Program
  4.2.1.2 Provides input and approval of project objectives, scope, and timeframes
  4.2.1.3 Assists in the definition of BC/DR roles and responsibilities
  4.2.1.4 Provides support and resources for BC/DR projects and the BC/DR Manager
  4.2.1.5 Provides high-level coordination and support during BC/DR plan development

 4.2.2 *Business Continuity / Disaster Recovery Manager*:
  4.2.2.1 Obtains BC/DR Steering Committee support for the BC/DR program, projects, and initiatives
  4.2.2.2 Gathers, researches, and reports information relevant to the BC/DR Program
  4.2.2.3 Organizes and provides oversight for BC/DR projects (defines objectives, assesses risk, plans details)
  4.2.2.4 Tracks and reports on project progress to the BC/DR Steering Committee
  4.2.2.5 Manages all organizational change requirements pertaining to BC/DR within OIT (e.g. culture, structure, mission & strategy, polices, processes)
  4.2.2.6 Coordinates, synchronizes, and facilitates general operations within the *OIT Emergency Operations Center*.

 4.2.3 Business Continuity / Disaster Recover Planning Team:
  4.2.3.1 Provides support to OIT BC/DR projects and external state organizations as required
  4.2.3.2 Individuals provide subject matter expertise from their functional areas throughout the development, implementation, and maintenance of the BC/DR program
  4.2.3.3 Develops BC/DR program guidelines, methodologies, standards, and best practices
  4.2.3.4 Ensures all BC/DR planning activity adhere to OIT policies, procedures, and standards

4.3 Declaration of a Disaster or Emergency Response

4.3.1   *Crisis Management Team* (CMT):
   4.3.1.1 Overall responsible for managing the crisis response
   4.3.1.2 Gathers facts and analyzes conditions regarding the crisis
   4.3.1.3 Allocates internal resources
   4.3.1.4 Coordinates with external agencies for required resources
   4.3.1.5 Coordinates OIT disaster response with external agencies
   4.3.1.6 Develops and controls communication plans and official external communications
   4.3.1.7 Manages and directs *Disaster Recovery Team(s)*

4.3.2   Disaster Recovery Team(s) (DRT):
   4.3.2.1 Responds to a disaster at the direction of the CMT
   4.3.2.2 Maintains proficiency in OIT BC/DR related procedures within their specialty areas
   4.3.2.3 Conducts damage assessments and documents/reports findings to CMT
   4.3.2.4 Provides for stabilization and resumption of operations after a disaster

5.0 <u>Directives</u>

5.1 The <u>Major Incident Procedure</u> sets command, control, and communication protocol.

5.2 Each OIT *Business Unit* must assign a representative to the *BC/DR Planning Team*. Representatives will provide current and comprehensive content for the OIT Business Continuity Plan (BCP) and will provide status updates on actions assigned to their area of responsibility. As applicable, some representatives will also be responsible for Disaster Recovery planning content to ensure that any damage or disruptions to critical assets (both within OIT and our customers within State Government) is mitigated and that these assets can be restored to normal or near-normal operations as quickly as possible.

5.3 OIT will use the ISO 22301:2012 standard for its BC/DR plan.

5.4 OIT will use the ISO 22317 standard for Business Impact Analysis.

5.5 The BC/DR plan will include procedures and support agreements to ensure on-time availability and delivery of required business functions and services.

5.6 The OIT Business Impact Analysis (BIA) and the Risk Assessment (RA) will be reviewed annually by the BC/DR Planning Team. Changes will be annotated as required based on any changes to the new business operating environment. The BIA and the RA will be certified by the BC/DR Manager and approved by the BC/DR Steering Committee.

5.7 BIAs and RAs may need to be reviewed before the annual review if there are major changes in the business environment that affect the data contained in the BIA and/or RA. The BC/DR Planning Team representatives are responsible for notifying the BC/DR Manager of any major changes that would require amendments to the BIA. The modified BIA and/or RA must be approved by the BC/DR Steering Committee.

5.8 The BC/DR plan must be certified annually by the BC/DR Manager and approved by the BC/DR Steering Committee.

5.9 The BC/DR Manager will prepare and present a bi-annual report to the BC/DR Steering Committee. The report will encompass the current status of BC/DR projects, initiatives, and overall readiness of the organization.

5.10 Resolution of issues in the development of, or support of, all OIT BC/DR plans, initiatives, and associated activities will be coordinated through the BC/DR Manager.

5.11 BC/DR compliance verification is managed by the BC/DR Manager with support from the BC/DR Planning Team. Each Business Unit must take appropriate action to address gaps identified in the Business Impact Analysis.

5.12 OIT Employees must participate in training exercises and drills as directed by the BC/DR Steering Committee.

5.13 OIT will conduct (at a minimum) two table top exercises annually as well as one operational exercise that includes simulated execution of the BC/DR Plan in a mock disaster scenario.

5.14 Restoration Priority Order (Based upon criteria established by the Governor's Office):
  5.14.1 Essential Communications
  5.14.2 Citizen Health & Safety
  5.14.3 Direct Citizen Services
  5.14.4 State Revenue
  5.14.5 Economic Development
  5.14.6 Routine Government Services

6.0 <u>Document Information</u>

Initial Issue Date: August 13, 2015
Latest Revision Date: October 2, 2017 – To update Document Information.

Point of Contact: Architecture-Policy Administrator, OIT
Approved By: Chief Information Officer, OIT

Appendix A – BC/DR Steering Committee Composition

The BC/DR Steering Committee meets quarterly to discuss BC/DR strategy, projects, resourcing, exercises, and tests and consists of the following members:

1. Chief Information Officer
2. Associate Chief Information Officer – Applications
3. Associate Chief Information Officer - Infrastructure
4. Director of Architecture & Policy
5. Director of Finance
6. Director of Project Management Office
7. Director of Technology Business Consultants

Appendix B – BC/DR Planning Team

The BC/DR Planning Team meets as directed by the BC/DR Manager and consists of the managers or designated representatives from select business units within OIT:

1. Applications Development
2. Client Technologies
3. Enterprise Architecture & Policy
4. Enterprise Security
5. Network Data Services
6. Network Radio Services
7. Network Voice Services
8. Operations Management
9. Project Management Office
10. Technology Business Consultants
11. UNIX, Oracle, DBA and Storage Team
12. Vendor Management Office
13. Windows Application & Hosting Group
14. Workforce Development