

<p style="text-align: center;"><b>NORTH CAROLINA DEPARTMENT OF COMMERCE</b></p>	<p style="text-align: center;"><b>Policy # MIS-11</b></p> <p style="text-align: center;"><b>TITLE: Business Continuity and Continuity of Operations Planning Policy</b></p>
	<p style="text-align: center;"><b>Administering Authority:</b></p> <p style="text-align: center;"><b>Management Information Systems</b></p>
<p><b>Effective Date: July 1, 2006</b></p> <p><b>Revisions: August 2011</b></p>	<p><b>Statutory Authority: EO 102, §) G.S. 147-33.89</b></p>

**1) Purpose** – Through the adoption of Business Continuity Management planning and execution, the North Carolina Department of Commerce (NC-DOC) will achieve its business continuity aim of safeguarding our reputation and public image. This will occur by adhering to NC Information Technology Services (ITS) directives and guidelines as well as industry best practices to meet the needs of staff, citizens, partners, and other critical stakeholders through ensuring that business critical support functions are not compromised by a major disruptive event. The Business Continuity Policy forms part of the risk management framework and Disaster Recovery Plan at NC-DOC.

**2) Scope** – This policy applies to the NC Department of Commerce, institutions, commissions, committees, boards, and divisions within the NC Department of Commerce under the purview of the Secretary.

**3) Policy** – NC-DOC must establish a Business Continuity Plan (BCP) to ensure business continuity for essential mission critical functions. The BCP must address both the general management aspects of the continuity process and those for Information Technology and data/voice communications elements. The BCP must include action plans for the reactivation of all essential services, and must include provision for loss of supply of services by those external agents upon which NC-DOC is critically dependant. On-going requirements for the BCP include, but are not limited to: ¾ Annual Risk Assessment review, including periodic maintenance of the Business Impact Analysis. ¾ Periodic update of the BCP to ensure currency of information, and response strategies. The plan must be reviewed for possible updating within 30 days of any major operational or system changes that will have a material effect on the contingency strategy of any NC-DOC entity. ¾ Training and evaluation purposes of the Business Continuity Plan each year or within 30 days of any major operational or system changes that will have a material effect on the contingency strategy of NC-DOC.

**Management responsibilities:** NC-DOC managers must ensure that those key functions for which they have responsibility can be satisfactorily performed following credible major disruptive events and that arrangements are in place to achieve this. This requires the proactive development, maintenance and devolution of business continuity planning within their areas. Managers are expected to encourage the active participation of staff in business continuity issues and must ensure that key personnel are able to perform competently during a major disruptive event.

NC-DOC Managers must:

- Complete a periodic Risk Assessment or more detailed Business Impact Analysis if requested.
- Manage risks in accordance with this policy
- Ensure that the Business Continuity Plan in their area of influence and control is exercised on schedule.

#### **4) Definitions:**

Business Continuity: Business continuity is “the uninterrupted availability of all key resources supporting essential business functions” (Australian National Audit Office, 2000)

Business Continuity Plans: A collection of procedures and information that is developed, compiled and maintained in readiness for use in the event of an emergency or disaster. (Associated terms: Business Recovery Plan, Disaster Recovery Plan, and Recovery Plan)

Business Continuity Management: Business Continuity Management provides for the availability of processes and resources in order to ensure the continued achievement of critical objectives.

Business Impact Analysis: A management level analysis, which identifies the impacts of losing organizational resources. The BIA measures the effect of resource losses and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk management and continuity management.

A major disruptive event: May be Natural (e.g. flood, hurricane, earthquake), Accidental (e.g. fire, contamination), Commercial (e.g. loss of supply of critical services) or Willful (e.g. sabotage, vandalism, arson, terrorism). Associated terms: “major crisis”, ‘disaster’.

Risk Assessment: The overall process of risk analysis and risk evaluation.

Stakeholders: Those people and organizations that may affect, or be affected by, or perceive themselves to be affected by, a decision or activity.

#### **5) Revision History –**