

DHHS POLICIES AND PROCEDURES MANUAL

Section VIII:	Security and Privacy
Title:	Security Manual
Chapter	Business Continuity and Disaster Recovery Plan(s)
Current Effective Date:	July 1, 2004
Revision History:	
Original Effective Date:	May 1, 2001

Purpose

This document provides guidance to DHHS Divisions and Offices for the development and management of IT business continuity and disaster recovery plans, and ensures that Information Technology Business Continuity Plans are in place to sustain the operations of critical information technology services to support the continuity of vital business functions.

Risk to the Organization

If business continuity or contingency plans are not available or are out of date, the DHHS division/offices may not be able to recover from a disaster or an extended outage in a reasonable amount of time. Under federal or state law, each DHHS division/office is obligated to have IT business continuity and IT disaster recovery plans to keep critical programs operating.

Policy

All DHHS Divisions and Offices shall develop, review and update information technology business continuity plans (BCP) and disaster recovery (DR) plans as part of an IT Business Continuity Management Program to ensure the timely and reliable access to critical automated business services.

Implementation

1. Each DHHS Division and Office shall complete business continuity plans and disaster recovery plans. The Division of Information Resource Management (DIRM)/DHHS Privacy and Security Office shall oversee the completion, revisions and implementation of the business continuity and disaster recovery plans. The plan(s) shall meet the specific business continuity requirements for each Division/Office.
2. Each DHHS Division/Office is responsible for developing and implementing division/office specific plans and procedures that adhere to this policy.
3. DHHS shall establish a Business Continuity (BC)/Disaster Recovery (DR) planning team to develop, administer and oversee the implementation of the overall Business Continuity Management Program. DIRM/DHHS Privacy and Security Office shall serve a manager of the DHHS IT Business Continuity Management Program.
 - A. Each Division/Office shall designate staff to participate on the team.
 - B. Unless otherwise designated by the Division/Office Director, the Division/Office Security Official shall serve on the team.
4. The BC/DR planning team shall do the following:
 - A. Evaluate the organization, managerial, and technical environments in which the BCP/DR plan(s) must be implemented.

- B. Identify the types of disasters most likely to occur and the resultant impacts on the agency's ability to perform its mission.
 - C. Propose protective measures to be implemented in anticipation of a natural or man-made disaster.
 - D. Coordinate the plan development in conjunction with other DHHS emergency response or disaster preparedness activities.
5. The Plan will result in an overall business continuity strategy that must include the development, maintenance, and testing of contingency plans and work around procedures to sustain operational continuity of mission critical information technology systems and resources. The plan development shall include periodic review, analysis and inclusion of practices that ensure compliance to applicable federal or state legislation, rules or conditions of funding specific to business continuity or disaster recovery. Plan(s) shall include:
- A. Establishment and identification of a Business Recovery Organization identifying roles and responsibilities, allocated resources and the scope of the business continuity management program.
 - B. Identification of mission critical information technology business systems and business functions as identified in the scope.
 - C. A business impact analysis that identifies time sensitive business functions, financial exposures, operational impacts that estimates total information technology resources necessary for successful business resumption.
 - D. A risk assessment to determine risk priorities and probability of identified risk.
 - E. Development and maintenance of current information technology business continuity and recovery plans, policies, and procedures.
 - F. Plan activation and notification procedures.
 - G. Communication Plan including crisis communication procedures and coordination with other applicable public authorities.
 - H. Emergency response procedures based upon type of emergency(s) and identify command and control procedures for the recovery operation.
 - I. Provision for the back up and replacement of information, equipment and staff resources, including work around procedures in the event of a disruption.
 - J. Identification of alternate locations, facilities and off-site storage facilities.
 - K. Identification of critical resources and inventories for plan implementation.
 - L. Development of recovery/restoration procedures for time critical systems/applications/functions and business functions.
 - M. Development of appropriate testing schedules to validate the information technology recovery plans and business operations recovery plans.
 - N. Development of training and awareness of the Business Continuity Program and plan(s).
 - O. Development of procedures to maintain and update at least annually the individual Division/Office and the comprehensive DHHS BC/DR plan(s).
 - P. Additional procedures or areas as deemed necessary by the Division/Office.
6. Each DHHS Division/Office shall submit the BCP/DRP on an annual basis to DIRM /DHHS Privacy and Security Office. DIRM shall submit, on behalf of DHHS, the BCPs and DRPs on an annual basis to the State Chief Information Officer.

Enforcement

Sanctions against Chapter 126 employees who fail to comply with the DHHS policies and/or agency procedures shall be in accordance with DHHS Disciplinary Action guidelines and related personnel policies except that the sanctions for educators subject to Chapter 115C of the North Carolina General States shall be in accordance with NCGS 115C-325 or 115C-287.1.

DHHS workforce members who do not fall under the categories above shall be subject to sanctions according to their written contract and/or state or federal civil and criminal regulations.

Exceptions

Requests for exceptions to this policy should be addressed the DHHS Security Officer (DHHS.Security@ncmail.net).

References

HIPAA Requirements

- 45 CFR 164.308 (a) (7) (ii) (A) Contingency planning documentation – Data Backup Plan
- 45 CFR 164.308 (a) (7) (ii) (B) Contingency planning documentation – Disaster Recovery Plan
- 45 CFR 164.308(a) (7) (ii) (C) Contingency planning documentation – Emergency Mode Operation Plan
- 45 CFR 164.308 (a) (7) (ii) (D) Contingency planning documentation – Testing and Revision Plan
- 45 CFR 164.308 (a) (7) (ii) (E) Contingency planning documentation – Data Criticality Analysis

Other Requirements

- NCGS 147-33.89,
- Information Resource Management Commission (IRMC) Policy “190, Aspects of Business Continuity Management
- ISO-15408 Information Technology – Security Techniques, Evaluation Criteria for IT Security, Part 2, Section 7, Class FRU, Resource Utilization
- ISO-17799 Code of Practice for Information Security Management, Section 11, Business Continuity Management
- CoBit: Governance, Control and Audit for Information and Related Technology

For questions or clarification on any of the information contained in this policy, please contact [DHHS Security Office](#). For general questions about department-wide policies and procedures, contact the [Office of Policy & Planning](#).