<Organization Name>	Information Security Contingency Planning Policy	
Department Name	Policy #	**Issue Date:** September 13, 2013
Approved by:		

1. Purpose

<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise Contingency Planning Policy, for managing risks from information asset disruptions, failures, and disasters through the establishment of an effective contingency planning program. The contingency planning program helps <Organization Name> implement security best practices with regard to enterprise business continuity and disaster recovery.

2. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <Organization Name>. Any information, not specifically identified as the property of other parties, that is transmitted or stored on <Organization Name> IT resources (including e-mail, messages and files) is the property of <Organization Name>. All users (<Organization Name> employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Intent

The <Organization Name> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a contingency planning capability throughout <Organization Name> and its business units to help the organization implement security best practices with regard to enterprise business continuity and disaster recovery.

4. Policy

<Organization Name> has chosen to adopt the Contingency Planning principles established in NIST SP 800-34 "Contingency Planning Guide for Federal Information Systems," as the official policy for this domain. The following subsections outline the Contingency Planning standards that constitute <Organization Name> policy. Each <Organization Name> Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- CP-1 Contingency Planning Procedures: All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented contingency planning procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- CP-2 Contingency Plan: All <Organization Name> Business Systems must develop a contingency plan for the company information assets that:
    - Identifies essential missions and business functions and associated contingency requirements.
    - Provides recovery objectives, restoration priorities, and metrics.

- Addresses contingency roles, responsibilities, assigned individuals with contact information.
- Addresses maintaining essential missions and business functions despite an information asset disruption, compromise, or failure.
- Addresses eventual, full information asset restoration without deterioration of the security measures originally planned and implemented.
- Is reviewed and approved by designated officials within the organization.
- Distributes copies of the contingency plan to relevant system owners and stakeholders.
- Coordinates contingency planning activities with incident handling activities.
- Reviews the contingency plan for the information asset on an **annual** basis.
- Revises the contingency plan to address changes to the organization, information asset, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
- Communicates contingency plan changes to relevant system owners and stakeholders.

- CP-3 Contingency Training: All <Organization Name> Business Systems must train personnel in their contingency roles and responsibilities with respect to the information asset and provide refresher training on an **annual** basis.
- CP-4 Contingency Plan Testing and Exercises: All <Organization Name> Business Systems must test and/or exercise the contingency plan for the information asset annually to determine the plan's effectiveness and the organization's readiness to execute the plan. In addition, <Organization Name> Business Systems must review the contingency plan test/exercise results and initiate corrective actions.
- CP-5 Alternate Storage Site: All <Organization Name> Business Systems must establish an alternate storage site including necessary agreements to permit the storage and recovery of information asset backup information.
- CP-6 Alternate Processing Site: All <Organization Name> Business Systems must establish an alternate processing site including necessary agreements to permit the resumption of information asset operations for essential missions and business functions within **defined recovery times and recovery points** when the primary processing capabilities are unavailable. In addition, <Organization Name> Business Systems will ensure that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.
- CP-8 Telecommunications Services: All <Organization Name> Business Systems must establish alternate telecommunications services including necessary agreements to permit the resumption of information asset operations for essential missions and business

functions within **defined recovery time and recovery points** when the primary telecommunications capabilities are unavailable.

- CP-9 Information System Backup: All <Organization Name> Business Systems must conduct backups of user-level, system-level, and information asset documentation (including security-related documentation) within **defined recovery time and recovery point objectives**. In addition, <Organization Name> Business Systems must protect the confidentiality and integrity of backup information at the storage location.
- CP-10 Information System Recovery and Reconstitution: All <Organization Name> Business Systems must provide for the recovery and reconstitution of the information asset to a known state after a disruption, compromise, or failure.

Appendix A – References

The following references illustrate public laws which have been issued on the subject of information security and should be used to demonstrate <Organization Name> responsibilities associated with protection of its information assets.

a. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems Revision 3, Operational Controls, Contingency Planning Control Family, August 2009.

b. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-34 "Contingency Planning Guide for Federal Information Systems" Revision 1 October 2009.

c. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-16 "Information Security Training Requirements: A Role- and Performance-Based Model" Revision 1 March 2009.

d. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 "Information Security Handbook: A Guide for Manager" October 2006.

e. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" September 2006.