EPA **IT/IM DIRECTIVE**
PROCEDURE

Information Security – Contingency Planning (CP) Procedure

Directive No: CIO 2150-P-06.3

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Contingency Planning (CP) Procedure

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Contingency Planning (CP) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

2. SCOPE

These procedures address all United States EPA information and information systems to include information and information systems used, managed, or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. BACKGROUND

EPA is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems. All EPA information systems shall meet security requirements by implementing the security controls defined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

5. AUTHORITY

Additional legal foundations for the Contingency Planning Procedure include:

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)

- OMB Circular A-130, “Managing Information as a Strategic Resource,” Appendix I, “Responsibilities for Protecting and Managing Federal Information Resources,” July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

6. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "CP" designator (e.g., CP-2, CP-3) identified for each procedure below corresponds to the NIST- identifier for the Contingency Planning control family, as identified in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

NIST defines the applicable CP security and privacy baseline controls in NIST 800-53B, Control Baselines for Information Systems and Organizations. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name.

CP-2 – Contingency Plan

For All Systems:

1) Develop a contingency plan for the system that:
   a) Identifies essential mission and business functions and associated contingency requirements;
   b) Provides recovery objectives, restoration priorities, and metrics;
   c) Addresses contingency roles, responsibilities, assigned individuals with contact information;
   d) Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
   e) Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
   f) Addresses the sharing of contingency information; and

g) Is reviewed and approved by the SO and ISO;

2) Distribute copies of the contingency plan to System Administrators (SA), Information Management Officer (IMO), Information Resource Management Branch Chief (IRMBC), and Continuity of Operations Plan (COOP) team as applicable;
3) Coordinate contingency planning activities with incident handling activities;
4) Review the contingency plan for the system annually or after significant changes to the system, such as, major upgrade to OS or critical software, and change in operating environment, i.e., moving from on-premise to cloud (or vice versa);
5) Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6) Communicate contingency plan changes to the SA, IMO, IRMBC, and COOP team as applicable;
7) Incorporate lessons learned from contingency plan testing, training or actual contingency activities into contingency testing and training; and
8) Protect the contingency plan from unauthorized disclosure and modification.

CP-2(1) – Contingency Plan | Coordinate with Related Plans

For Moderate and High Systems:

1) Coordinate contingency plan development with organizational elements responsible for related plans.

CP-2(2) – Contingency Plan | Capacity Planning

For High Systems:

1) Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

CP-2(3) – Contingency Plan | Resume Mission and Business Functions

For Moderate and High Systems:

1) Plan for the resumption of essential mission and business functions within recovery objectives, specified in the Contingency Plan, Business Impact Analysis (BIA) or COOP planning documents of contingency plan activation.

CP-2(5) – Contingency Plan | Continue Mission and Business Functions

For High Systems:

1) Plans for the continuance of essential mission and business functions or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

CP-2(8) – Contingency Plan | Identify Critical Assets

For Moderate and High Systems:

1) Identify critical system assets supporting essential mission and business functions.

CP-3 – Contingency Training

For All Systems:

1) Provide contingency training to system users consistent with assigned roles and responsibilities:
    a) Within thirty (30) days of assuming a contingency role or responsibility;
    b) When required by system changes; and
    c) Annually thereafter, and
2) Review and update contingency training content annually and following significant changes to the system.

CP-3(1) – Contingency Training | Simulated Events

For High Systems:

1) Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

CP-4 – Contingency Plan Testing

For All Systems:

1) Test the contingency plan for the system prior to a new system going live and annually thereafter or after significant changes using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through, table-top exercises, simulated or live exercises.
2) Review the contingency plan test results; and
3) Initiate corrective actions, if needed.

CP-4(1) – Contingency Plan Testing | Coordinate with Related Plans

For Moderate and High Systems:

1) Coordinate contingency plan testing with organizational elements responsible for related plans.

CP-6 – Alternate Storage Site

For Moderate and High Systems:

1) Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

2) Ensure the alternate storage site provides controls equivalent to that of the primary site.

CP-6(1) – Alternate Storage Site | Separation from Primary Site

For Moderate and High Systems:

1) Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

CP-6(2) – Alternate Storage Site | Recovery Time and Recovery Point Objectives

For High Systems:

1) Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

CP-6(3) – Alternate Storage Site | Accessibility

For Moderate and High Systems:

1) Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-7 – Alternate Processing Site

For Moderate and High Systems:

1) Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of information system operations necessary for essential mission and business functions within the Recovery Time Objective (RTOs) and Recovery Point Objectives (RPOs) established in the Contingency Plan and BIA when the primary processing capabilities are unavailable;
2) Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
3) Provide controls at the alternate processing site that are equivalent to those at the primary site.

CP-7(1) – Alternate Processing Site | Separation from Primary Site

For Moderate and High Systems:

1) Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

CP-7(2) – Alternate Processing Site | Accessibility

For Moderate and High Systems:

1) Identify potential accessibility problems to the alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7(3) – Alternate Processing Site | Priority of Service

For Moderate and High Systems:

1) Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

CP-7(4) – Alternate Processing Site | Preparation for Use

For High Systems:

1) Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

CP-8 – Telecommunications Services

For Moderate and High Systems:

1) Establish alternate telecommunications services, including necessary agreements to permit the resumption of information system services or operations including all data, telecom, and networking services and operations for essential mission and business functions within the RTOs established in the Contingency Plan or BIA when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8(1) – Telecommunications Services | Priority of Service Provisions

For Moderate and High Systems:

1) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and
2) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8(2) – Telecommunications Services | Single Points of Failure

For Moderate and High Systems:

1) Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-8(3) – Telecommunications Services | Separation of Primary and Alternate Providers

For High Systems:

1) Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

CP-8(4) – Telecommunications Services | Provider Contingency Plan

For High Systems:

1) Require primary and alternate telecommunications service providers to have contingency plans;
2) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and
3) Obtain evidence of contingency testing and training by providers annually and upload into the Governance, Risk and Compliance (GRC) tool as an artifact.

CP-9 – System Backup

For All Systems:

1) Conduct backups of user-level information contained in the information system components such as hard drives, network file storage, cloud storage at least weekly consistent with the RTO and RPO;
2) Conduct backups of system-level information contained in the system at least weekly consistent with the RTO and RPO;
3) Conduct backups of system documentation, including security-and privacy related documentation at least weekly consistent with the RTO and RPO; and
4) Protect the confidentiality, integrity, and availability of backup information.

CP-9(1) – System Backup | Testing for Reliability and Integrity

For Moderate and High Systems:

1) Test backup information at least quarterly to verify media reliability and information integrity.

CP-9(2) – System Backup | Test Restoration Using Sampling

For High Systems:

1) Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

CP-9(3) –System Backup | Separate Storage for Critical Information

For High Systems:

1) Store backup copies of critical system software and security-related information necessary for the system to perform its function or mission in a separate facility or in a fire rated container that is not collocated with the operational system.

CP-9(5) – System Backup | Transfer to Alternate Storage Site

For High Systems:

1) Transfer system backup information to the alternate storage site on a monthly basis and transfer rate consistent with system specific RTO and RPO.

CP-9(8) – System Backup | Cryptographic Protection

For All Systems:

1) Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of system backup information in storage, at rest, and in transit at both primary and alternate locations.

CP-10 – System Recovery and Reconstitution

For All Systems:

1) Provide for the recovery and reconstitution of the system to a known state within recovery objectives, specified in the Contingency Plan after a disruption, compromise, or failure.

CP-10(2) – System Recovery and Reconstitution | Transaction Recovery

For Moderate and High Systems:

1) Implement transaction recovery for systems that are transaction-based.

CP-10(4) – System Recovery and Reconstitution | Restore Within Time Period

For High Systems:

1) Provide the capability to restore information system components within the RTOs and RPOs specified in the Contingency Plan from configuration-controlled and integrity-protected information representing a known, operational state for the components.

7. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

8. RELATED INFORMATION

The information listed below relates to the Contingency Planning Procedure.

- NIST Special Publications 800-34, Contingency Planning Guide for Information Technology Systems

9. DEFINITIONS

Definitions which pertain to the Information Security - Contingency Planning Procedures are listed below.

- **After Action Report** – a document containing findings and recommendations from an exercise, test, or analysis of an actual disruption or failure and the response to and recovery from it.
- **Alternate Processing Site** – a facility that is able to support system operations by restoring critical systems to an acceptable level as defined in the Disaster Recovery Plan. Sites are referred to as cold, warm, hot, mobile, or mirrored.
- **Alternate Storage Site** – a secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored.
- **Availability** – ensuring timely and reliable access to and use of information.
- **Business Continuity Plan (BCP)** – the documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.
- **Business Impact Analysis (BIA)** – an analysis of an information system's requirements, processes and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
- **Confidentiality** – preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- **Contingency Training** – the dynamic development and implementation of a coordinated training strategy for contingency personnel on information systems or applications' CPs.
- **Continuity of Support Plan/IT Contingency Plan (CP)** – management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. From the standpoint of information systems, a CP is the documentation of a predetermined set of instructions or procedures that describes how to sustain operations in the event of a significant disruption.
- **Continuity of Operations Plan (COOP)** – a predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.
- **Disaster Recovery Plan (DRP)** – a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

- **Incident** – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- **Incident Response Plan** – the documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of a malicious cyber-attack against an organization's IT systems.
- **Information Security** – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.
- **Information System** – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- **Integrity** – guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- **Maximum Tolerable Downtime (MTD)** – the total amount of time the SO/Authorizing Official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.
- **Media** – physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks and Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored or printed within an information system. Digital media include diskettes, tapes, removable hard drives, flash/thumb drives, compact disks and digital video disks. Examples of non-digital media are paper or microfilm. This term also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).
- **National Security Emergency Preparedness (NSEP) Telecommunications Services** – telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NSEP posture of the United States. These services fall into two specific categories, Emergency NSEP and Essential NSEP and are assigned priority levels pursuant to Section 9 of 47 C.F.R. Pt. 64, App. A.
- **Organization** – a federal agency or, as appropriate, any of its operational elements.
- **Reconstitution** – takes place following recovery and includes activities for returning the information system to its original functional state before CP activation.
- **Recovery** – executing information system CP activities to restore essential missions and business functions.
- **Recovery Point Objective (RPO)** – the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage.
- **Recovery Time Objective (RTO)** – the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business functions and the MTD.

- **Risk** – the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- **Service Level Agreement (SLA)** – part of a service contract in which a certain level of service is agreed upon. An SLA is not a type of service contract, but rather a part of a service contract. A service contract can contain zero, one or more SLAs. A contract containing SLAs is usually referred to as a performance contract.
- **Signature** (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation (can be accomplished manually, sometimes referred to as a "wet signature," or electronically).
- **Significant Change** – a change that is likely to substantively affect the security or privacy posture of a system.
- **Telecommunications Service Priority (TSP)** – a program that provides NSEP users priority authorization in restoring or establishing telecommunications services that are vital to coordinating and responding to crises. A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service.
- **User** – individual or (system) process authorized to access an information system.
- **Vital Records** – also termed Essential Records -- Records essential to the continued functioning or reconstitution of an organization during and after an emergency in addition to those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.
- **Written** (or in writing) – to officially document the action or decision, either manually or electronically and includes a signature.

10. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

11. MATERIAL SUPERSEDED

Information Directive: CIO 2150-P-06.2, Information Security – Contigency Planning Procedures

12. CONTACTS

For further information, please contact the OMS, Office of Information Security and Privacy (OISP).

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.06.12 08:18:08 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information
and Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

BIA	Business Impact Analysis
BCP	Business Continuity Plan
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
CP	Contingency Plan
DRP	Disaster Recovery Plan
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
LSI	Large-Scale Integration
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
NSEP	National Security Emergency Preparedness
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OMS	Office of Mission Support
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIO	Senior Information Official
SLA	Service Level Agreement
SO	System Owner
SP	Special Publication
TSP	Telecommunications Service Priority
U.S.C.	United States Code