Policy and Procedure 9-6
Information Technology: Contingency Planning

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	6/5/2024
Effective Date:	June 3, 2024		
Codes/Mandates:	Code of Virginia: §2.2-2007 and Code of Virginia, §2.2-2005		
References:	Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00, ITRM Standard SEC530: Information Security Standard, ITRM Standard SEC502: Audit Security Standard		
Forms:	N/A		

CONTENTS

PURPOSE

The purpose of this policy and procedure is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that Department of Forestry develops, disseminates, and updates the IT Contingency Planning Policy. This policy and procedure establishes the minimum requirements for the Information Technology Contingency Planning Policy and Procedure.

This policy and procedure is intended to meet the control requirements outlined in SEC530, Section 8.6 Contingency Planning Family, Controls CP-1 through CP-11, to include specific requirements for the Commonwealth of Virginia.

SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as all Department of Forestry systems classified as sensitive.

DEFINITIONS and ACRONYMS

"Agency" and **"DOF"** means the Virginia Department of Forestry.

"Data owner" means the agency manager or supervisor, designated by the state forester, who defines, manages and controls the use of data and ensures compliance with adopted standards.

"Information security officer" and **"ISO"** means the agency employee who is designated by the state forester to develop and manage the agency's information security program, as required in the Commonwealth's Information Security Standard, SEC530.

"System administrator" means the agency employee who implements, manages, and/or operates a system at the direction of the system owner or data owner.

"System owner" means the agency manager or supervisor who is responsible for the operation and oversight of any given agency business system.

ACRONYMS

BIA:	Business Impact Analysis
CIO:	Chief Information Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
DOF:	Department of Forestry
DRP:	Disaster Recovery Plan
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
RA:	Risk Assessment
RPO:	Recovery Point Objective
RTO:	Recovery Time Objective
SEC530:	Information Security Standard 530
VDEM:	Virginia Department of Emergency Management
VITA:	Virginia Information Technology Agency

BACKGROUND

The Information Technology Contingency Planning Policy and Procedure at is intended to facilitate the effective implementation of the processes necessary to meet the contingency planning requirements as stipulated by the COV ITRM Security Standard SEC530 and security best practices. This policy and procedure directs the Department of Forestry to meet these requirements for all sensitive IT systems.

ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibility as described in the Statement of Process section. The following Roles and Responsibility Matrix describes 4 role specific activities:

- Responsible (R) – Person working on activity
- Accountable (A) – Person with decision authority and one who delegates the work
- Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
- Informed (I) – Person who needs to know of decision or action

Roles	Users	User Supervisor	System Owner	System Admin	Human Resource Manager	Information Security Officer
Tasks						
Designate an employee to focus on the it continuity plan and work with the Department of Forestry continuity coordinator.						A

Identify mission essential functions (mefs) and business essential functions (befs).	I	R	C	C		A
Identify recovery time objectives (rto), recovery point objectives (rpo) and metrics	I	R	C	C		A
Develop IT components of Department of Forestry continuity plan, annual exercise, exercise review and plan revision		R				A
Identify contingency roles and responsibilities assignments, contact information, delegations of authority, orders of succession and notification procedures.	I	R				A
Approve IT disaster recovery plan.	A	I			R	R
Establish communication methods to support it system users for essential functions.		R			R	A
Require training of IT disaster recovery staff.		R			R	A
Develop contingency plan.	I	R			R	A
Distribute contingency plan.	I	R				A
Review and revise contingency plan.	I	R			R	A
Coordinate contingency plan development.	I	R				A
Conduct capacity planning.	I	R			R	A
Train personnel in contingency roles.	I	R				A
Test contingency plan.	I	R			R	A
Identify and configure alternate storage site.	I	R			R	A
Identify and configure alternate processing site.	I	R			R	A
Establish alternate telecommunications services.	I	R			R	A
Conduct information system backups.		I	R	R	R	A
Implement service provider system backup plans.		R	I	I		A
Information system recovery and reconstitution.		R	I	I	R	A
Implement transaction recovery.		R	I	I	R	A

STATEMENT OF POLICY

In accordance with SEC530, CP-1 through CP-11, Department of Forestry will be responsible to ensure that a Continuity Plan (previously referred to as Continuity of Operations Plan or COOP, to include an IT Disaster Recovery Plan, if applicable) is developed and maintained to include procedures to recover all mission essential Department of Forestry functions and resume normal business activities after an interruption.

POLICY AND PROCEDURES (CP-1)

Essential functions are determined through the Business Impact Analysis (BIA), a process of identifying and prioritizing the essential functions of an agency and measuring the impact that results from a loss or prolonged interruption of these operations. The BIA also identifies the resources required to support these essential functions. The Department of Forestry BIA should be a primary input to the Department of Forestry Continuity Planning process.

1. The ISO or IT director shall:

    a. Collaborate with the continuity plan coordinator as the focal point for IT aspects of continuity and related disaster recovery (DR) planning activities;

- **Note:** Designation of an agency continuity plan coordinator is included in the continuity planning requirements issued by VDEM.

b. Based on BIA and RA results, develop IT disaster components of Department of Forestry's Continuity Plan which identifies:

   i. Each IT system that is necessary to recover essential business functions or dependent business functions and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each; and

   ii. Personnel contact information and incident notification procedures.

- **Note:** If the Continuity Plan contains sensitive data, those components with sensitive data should be protected and stored at a secure off-site location.

c. Require an annual exercise (or more often as necessary) of IT Disaster Recovery components to assess their adequacy and effectiveness.

d. Require review and revision of IT Disaster Recovery components following the exercise (and at other times as necessary).

e. Based on the Continuity Plan, develop and maintain an IT Disaster Recovery Plan, which supports the restoration of essential business functions and dependent business functions.

f. Require approval of the IT Disaster Recovery Plan by the agency head.

g. Require annual review, reassessment, testing and revision of the IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel.

h. Establish communication methods to support IT system users' local and remote access to IT systems and data that support essential business functions, as necessary.

i. Require training of all IT Disaster Recovery Plan team members in their Disaster Recovery responsibilities.

Contingency Plan (CP-2)

Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised.

1. ISO or designee shall:

   a. Develop a contingency plan for the information system that:

      i. Identifies essential missions and business functions and associated contingency requirements.

      ii. Provides recovery objectives, restoration priorities, and metrics.

      iii. Addresses contingency roles, responsibilities, assigned individuals with contact information, including delegations of authority, orders of succession, and notification procedures.

      iv. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.

         - Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack.

      v. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented, including devolution and reconstitution.

      vi. Is reviewed and approved by the Information Security Officer.

      vii. Addresses alternate facilities, interoperable communications, vital records, human capital management and requirements for tests, training and exercises.

   b. Distribute copies of the contingency plan to organization-defined key contingency personnel (identified by name and/or by role) and organizational elements.

c. Coordinate contingency planning activities with incident handling activities.

d. Review the contingency plan for the information system at least once a year or more frequently if needed to address an environmental change.

e. Revise the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution or testing.

f. Communicate contingency plan changes to the organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements.

g. Coordinate contingency plan development with organizational elements responsible for related plans, for example, Business Continuity Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan and Occupant Emergency Plan.

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

i. Plan for the resumption of essential missions and business functions within the organization-defined time period of contingency plan activation.

j. Plan for the continuance of essential mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

k. Plan for the transfer of essential mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

l. Coordinate DOF contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

m. Identify critical system assets supporting all mission and business functions.

n. Protect the contingency plan from unauthorized disclosure and modification.

Contingency Training (CP-3)

1. The ISO or designee shall provide contingency training to system users consistent with assigned roles and responsibilities:

   a. Within 30-days of assuming a contingency role or responsibility

   b. When required by system changes

   c. Annually thereafter

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

2. Review and update contingency training content annually and following environmental change.

Contingency Plan Testing (CP-4)

1. The ISO or designee shall:

   a. Test the contingency plan for the system at least on an annual basis and following an environmental change using organization-defined tests to determine the effectiveness of the plan and the readiness to execute the plan.

   b. Review the contingency plan test results.

   c. Initiate corrective actions, if needed.

   d. Coordinate contingency plan testing and/or exercises with organizational elements responsible for related plans, for example, Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis

Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.

e. Test/exercise the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

f. Include a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Alternate Storage Site (CP-6)

1. The ISO or designee shall:

   a. Establish an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.

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

   c. Identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.

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

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

   - **Note:** Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.

Alternate Processing Site (CP-7)

2. The ISO or designee shall:

   a. Establish an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the organization-defined time period consistent with recovery time objectives when the primary processing capabilities are unavailable.

   b. 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.

   c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

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

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

   f. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements (including RTOs);

   g. Prepare the alternate processing site so that it is ready to be used as the operational site supporting essential mission and business functions.

   h. Plan and prepare for circumstances that preclude returning to the primary processing site.

Telecommunications Services (CP-8)

1. The ISO or designee shall establish alternate telecommunication services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within 24 hours when

the primary telecommunication capabilities are unavailable at either the primary or alternate processing or storage sites including the following provisions:

a. Develop primary and alternate telecommunication service agreements that contain priority of- service provisions in accordance with the organization's availability requirements.

b. Request Telecommunication Service Priority for all telecommunication services used for national security emergency preparedness in the event that the primary and/or alternate telecommunication services are provided by a common carrier.

c. Obtain alternate telecommunication services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunication services.

d. Obtain alternate telecommunication service providers that are separated from primary service providers to reduce susceptibility to the same threats.

e. Require primary and alternate telecommunication service providers to have contingency plans.

f. Review provider contingency plans to ensure that the plans meet organizational contingency requirements.

g. Obtain evidence of contingency testing and training by providers on a frequency defined by the organization.

System Backup (CP-9)

1. The system and/or data owner shall:

   a. Conduct backups of user-level information contained in the information system within the organization-defined frequency consistent with recovery time and recovery point objectives.

   b. Conduct backups of system-level information contained in the information system in accordance with organization-defined frequency consistent with recovery time and recovery point objectives, including system-state information, operating system and application software and licenses.

   c. Conduct backups of system documentation including security and privacy-related documentation in accordance with organization-defined frequency consistent with recovery time and recovery point objectives.

   d. Protect the confidentiality and integrity of backup information.

   e. Test backup information at least every 30-days to verify media reliability and information integrity.

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

   g. Store backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

   h. Transfer system backup information to the alternate storage site at least on a daily basis or sooner based on organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives.

   i. Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

   j. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of sensitive backup information.

   k. For every IT system identified as sensitive relative to availability, the ISO or designee shall or shall require that its service provider implement backup and restoration plans to support restoration of systems, data and applications in accordance with Department of Forestry requirements. At a minimum, these plans shall address the following:

      i. Secure off-site storage for backup media.

ii. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.

iii. Performance of backups only by authorized personnel.

iv. Review of backup logs after the completion of each backup job to verify successful completion.

v. Approval of backup schedules of a system by the system owner.

vi. Approval of emergency backup and operations restoration plans by the system owner.

vii. Protection of any backup media that is sent off-site (physically or electronically) or shipped by the United States Postal Service or any commercial carrier, in accordance with Department of Forestry requirements.

viii. Authorization and logging of deposits and withdrawals of all media that is stored off-site.

ix. Retention of the data handled by an IT system in accordance with Department of Forestry's records retention policy.

x. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.

xi. Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form.

xii. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures, in accordance with Department of Forestry's Continuity of Operations Plan.

System Recovery and Reconstitution (CP-10)

1. The ISO or designee provides for the recovery and reconstitution of the information system to a known state within organization-defined time period consistent with recovery time and recovery point objectives after a disruption, compromise or failure.

a. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation.

b. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives and appropriate metrics.

c. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations.

d. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise or failure.

e. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures.

2. The system administrator shall implement transaction recovery for systems that are transaction-based using transaction rollback, transaction journaling or similar mechanism.

3. DOF shall provide the capability to reimage information system components within the organization-defined restoration time-periods from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

4. DOF shall protect system components used for recovery and reconstitution (i.e., hardware, firmware and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilers and other system software.

Alternate Communications Protocols (CP-11)

The ISO or designee provides the capability to employ organization-defined alternative communications protocols in support of maintaining continuity of operations.

AUTHORITY

This policy and procedure is issued by the Virginia state forester.

INTERPRETATION

The director of information technology and the chief of administration are responsible for the interpretation of this policy and procedure.

APPROVAL

I certify that this policy and procedure is approved and ready for publication.

Parik Patel	DocuSigned by: Parik Patel 3448F7C5358F457... 6/5/2024
Director of Information Technology Name (Print)	Director of Information Technology Signature
Amanda Davis	DocuSigned by: amanda davis C2CCAB60F85A4A6... 6/5/2024
Chief of Administration Name (Print)	Chief of Administration Signature

Version History

Version History			
Date	**Version**	**Details**	**Author/Contributors**
June 3, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO