**IT Contingency Planning Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the IT Contingency Planning Policy. This policy and procedure establishes the minimum requirements for the IT Contingency Planning Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.6 Contingency Planning Family, Controls CP-1 through CP-10, to include specific requirements for the Commonwealth of Virginia.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems classified as sensitive.

# ACRONYMS

BIA: Business Impact Analysis

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

DRP: Disaster Recovery Plan

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

RA: Risk Assessment

RPO: Recover Point Objective

RTO: Recovery Time Objective

SEC501: Information Security Standard 501

VDEM: Virginia Department of Emergency Management

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The IT Contingency Planning Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the contingency planning requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all sensitive IT systems.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Roles** | Agency Head | IT Continuity/DR Designee | Data Owner | System Owner | Security Operations Staff | Information Security Officer |
| **Tasks** |  |  |  |  |  |  |
| Designate an employee to focus on the it continuity plan and work with the “YOUR AGENCY NAME” 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 “YOUR AGENCY NAME” continuity plan, annual exercise, exercise review and plan revision |  | R |  |  |  | A |
| Contingency roles and responsibilities assignments, contact information, delegations of authority, orders of succession and notification procedures | I | R |  |  |  | A |
| Approve it dr plan | A | I |  |  | R | R |
| Establish communication methods to support it system users for essential functions |  | R |  |  | R | A |
| Require training of it dr 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 |
| Contingency plan testing | 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 SEC501, CP-1 through CP-10, “YOUR AGENCY NAME” 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 “YOUR AGENCY NAME” functions and resume normal business activities after an interruption.

1. **CONTINGENCY PLANNING POLICY AND PROCEDURES**

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 “YOUR AGENCY NAME” BIA should be a primary input to the “YOUR AGENCY NAME” Continuity Planning process.

* 1. The ISO or designee shall:
     1. Designate an employee to collaborate with “YOUR AGENCY NAME”’s 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.

* + 1. Based on BIA and RA results, develop IT disaster components of “YOUR AGENCY NAME”’s Continuity Plan which identifies:
       1. 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
       2. 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.

* + 1. Require an annual exercise (or more often as necessary) of IT DR components to assess their adequacy and effectiveness;
    2. Require review and revision of IT DR components following the exercise (and at other times as necessary);
    3. Based on the Continuity Plan, develop and maintain an IT DRP, which supports the restoration of essential business functions and dependent business functions;
    4. Require approval of the IT DRP by the Agency Head;
    5. Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel;
    6. Establish communication methods to support IT system users’ local and remote access to IT systems and data that support essential business functions, as necessary; and
    7. Require training of all IT DRP team members in their Disaster Recovery responsibilities.

1. **CONTINGENCY PLAN**

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. The ISO or designee shall:
     1. Develop a contingency plan for the information system that:
        1. Identifies essential missions and business functions and associated contingency requirements;
        2. Provides recovery objectives, restoration priorities, and metrics;
        3. Addresses contingency roles, responsibilities, assigned individuals with contact information, including delegations of authority, orders of succession, and notification procedures;
        4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
           1. 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.
        5. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented, including devolution and reconstitution;
        6. Is reviewed and approved by designated officials within the “YOUR AGENCY NAME”; and
        7. Addresses alternate facilities, interoperable communications, vital records, human capital management, and requirements for tests, training, and exercises.
     2. Distribute copies of the contingency plan to an organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements;
        1. After developing the “YOUR AGENCY NAME” Continuity Plan, the ISO and “YOUR AGENCY NAME” Continuity Coordinator shall communicate “YOUR AGENCY NAME”’s recovery requirements for enterprise IT systems and data to the Northrop Grumman Partnership. For non-enterprise systems, the IT recovery requirements will be communicated to the business owners.
     3. Coordinate contingency planning activities with incident handling activities;
     4. Review the contingency plan for the information system at least once a year;
     5. 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;
     6. Communicate contingency plan changes to the organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements;
     7. 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;
        1. The ISO and “YOUR AGENCY NAME” Continuity Coordinator shall obtain approval of the Partnership IT DRP by the Chief Information Officer of the Commonwealth (CIO). In addition, the ISO and “YOUR AGENCY NAME” Continuity Coordinator shall coordinate periodic review, reassessment, and revision of the IT DRP with the Partnership, in order to reflect changes in mission essential and essential business functions, services, IT system hardware and software, and personnel.
     8. Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations; and
     9. Plan for the resumption of essential missions and business functions within the organization-defined time period of contingency plan activation.

1. **CONTINGENCY TRAINING**
   1. The ISO or designee shall train personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training at least once a year or within 30-days of a role or assignment change.
      1. Contingency training incorporates simulated events effective response by personnel in crisis situations.
2. **CONTINGENCY PLAN TESTING AND EXERCISES** 
   1. The ISO or designee shall:
      1. Test and/or exercise the contingency plan for the information system at least once a year or when the contingency plan is revised using an organization-defined tests and/or exercises to determine the plan’s effectiveness and the organization’s readiness to execute the plan;
         1. Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.
      2. Review the contingency plan test/exercise results and initiates corrective actions;
      3. 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;
      4. 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; and
      5. Include a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.
3. **ALTERNATE STORAGE SITE**
   1. The ISO or designee shall:
      1. Establish an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information;
      2. Identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards;
      3. Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives; and
      4. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
         1. 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.
4. **ALTERNATE PROCESSING SITE** 
   1. The ISO or designee shall:
      1. 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;
      2. 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;
      3. Identify an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards;
      4. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions;
      5. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with the organization’s availability requirements;
      6. Configure the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions; and
      7. Ensures that the alternate processing site provides information security measures equivalent to that of the primary site.
5. **TELECOMMUNICATIONS SERVICES**
   1. The ISO or designee shall establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable, including the following requirements for sensitive systems:
      1. Develop primary and alternate telecommunications service agreements that contain priority of- service provisions in accordance with the organization’s availability requirements;
      2. Request Telecommunications Service Priority for all telecommunications services used for emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier;
      3. Obtain alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services;
      4. Obtain alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards; and
      5. Require primary and alternate telecommunications service providers to have contingency plans.
6. **INFORMATION SYSTEM BACKUP**
   1. The System and/or Data Owner shall:
      1. Conduct backups of user-level information contained in the information system within the organization-defined frequency consistent with recovery time and recovery point objectives;
      2. 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;
      3. Conduct backups of information system documentation including security-related documentation in accordance with organization-defined frequency consistent with recovery time and recovery point objectives;
      4. Protect the confidentiality and integrity of backup information at the storage location using digital signatures, cryptographic hashes or similar mechanisms;
      5. Test backup information at least every 30-days to verify media reliability and information integrity;
      6. Use a sample of backup information in the restoration of selected information system functions as part of contingency plan testing; and
      7. 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.
   2. 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 “YOUR AGENCY NAME” requirements. At a minimum, these plans shall address the following:
      1. Secure off-site storage for backup media.
      2. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.
      3. Performance of backups only by authorized personnel.
      4. Review of backup logs after the completion of each backup job to verify successful completion.
      5. Approval of backup schedules of a system by the System Owner.
      6. Approval of emergency backup and operations restoration plans by the System Owner.
      7. 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 “YOUR AGENCY NAME” requirements.
      8. Authorization and logging of deposits and withdrawals of all media that is stored off-site.
      9. Retention of the data handled by an IT system in accordance with “YOUR AGENCY NAME”’s records retention policy.
      10. 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.
      11. 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.
      12. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures, in accordance with “YOUR AGENCY NAME”’s Continuity of Operations Plan.
7. **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION**
   1. The ISO or designee provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
      1. Recovery is executing information system contingency plan activities to restore essential missions and business functions.
      2. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation.
      3. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics.
      4. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations.
      5. 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.
      6. 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. The ISO or designee shall provide compensating security controls for those organization-defined circumstances that can inhibit recovery and reconstitution to a known state.
   4. “YOUR AGENCY NAME” 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.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO” ““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

[ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History | | |
| --- | --- | --- |
| Version | Date | Change Summary |
| 1 | 01/13/2004 | Original document. |
| 2 | 09/28/2007 | Supersedes v1. Changes include update to IT Security Standard (SEC501-01) and addressing the responsibilities of “YOUR AGENCY NAME” Commonwealth Security & Risk Management (CSRM) Directorate and the “YOUR AGENCY NAME” COOP Coordinator. |
| 3 | 03/01/2013 | Administrative Changes |
| 4 | 07/01/2014 | Complete rewrite of Business Continuity Policy based on Information Security Standard SEC501 Revision 8 with Role Matrix added. |
| 5 | 11/15/2021 | Formatting changes |