



District of Columbia Pretrial Services Agency

Policy Statement 5556

**Policy Area: Information Technology
Effect**

Approved: _____

Ronald L. Hickey
Director, OIT

Management Instruction

CONTINGENCY PLANNING CONTROL FOR PSA BUSINESS AND MISSION CRITICAL SYSTEMS

I. MANAGEMENT INSTRUCTION

The District of Columbia Pretrial Services Agency's (PSA) business and mission critical systems must be supported by adequate contingency planning controls. The controls are required to be implemented and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5506, *Contingency Planning Policy for PSA Business and Mission Critical Systems*.

II. COVERAGE

This Management Instruction applies to all permanent and temporary PSA employees, including contractors and interns that use, manage, develop, maintain, or support PSA business and mission critical systems. The term employee as used in this management instruction, collectively refers to all of the aforementioned personnel types.

III. BACKGROUND

Contingency planning minimizes risk to PSA operations by planning for and proving the capability to recover and reconstitute the agency's business and mission critical systems should a disruption or disaster occur.

Loss, disruption, or prevention from access to processing, storage, or communications capacity for an extended duration can be caused by power outage, hardware failure, fire, natural disaster, terrorism, inadvertent data loss or system malfunction. Planning for recovery and/or reconstitution from these events is essential.

IV. PROCEDURES

A. Definitions

This Management Instruction outlines procedures for adequate contingency planning supported by process and technology. Contingency planning is the identification, preservation, and appropriation of people, process, technology, and material required to restore mission support operations provided by PSA's business and mission critical systems, infrastructure and systems support personnel in the event of a disruption or disaster.

B. Terms

- **Alternate Processing Site** – Pre-identified and contractually arranged alternate facilities to be used in the event of system disruption or in response to disaster recovery and continuity of support.
- **Backup** - Copy of critical system data, operational data, and documentation to a separate storage medium (e.g., tape).
- **Configuration Settings** – Functional and physical characteristics of hardware or software.
- **Continuity of Support Plan and Disaster Recovery Plan (COS/DR Plan)** – Detailed plan identifying the people, process, responsibilities, technology, and logistics required for planning for and recovering from disaster or disruption and for providing continued mission support.
- **Data Center** - Centralized physical environs of servers and associated support equipment
- **Priority of Service** – Legal contract with a service provider, guaranteeing priority over other government or commercial entities in the event of an excess of demand on the provider.
- **Restoration** – Process of restoring system and operational hardware, software, configuration settings, and operational processes to an acceptable state.
- **Service Restoration Team** – PSA IT staff and/or contractors who are responsible for restoring systems at the alternate site.
- **System Patches** - Software updates released by a software manufacturer to fix bugs or security holes in existing operating systems and/or applications.
- **Telecommunication Service** – Service for establishing and enabling transport of information, including data, text, pictures, voice and video.

C. Authority

The Federal Information Security Management Act (FISMA) requires PSA to institute procedures to facilitate the implementation of a Contingency Planning Policy. The procedures are derived from guidance provided by the National

Institute of Standards and Technology Special Publication 800-53, Draft 2,
Recommended Security Controls For Federal Information Systems.

D. Requirements

The following contingency planning procedures are required to be implemented, practiced, and monitored as described in this Management Instruction, and as mandated and authorized by PSA Policy Statement #5506, *Contingency Planning Policy For PSA Business and Mission Critical Systems.*

The following technical and process requirements meet the minimum baseline for systems with a security categorization of *Moderate*. Deviations from, or enhancements to these baseline procedures, will be documented, with rationale (e.g., mitigating factors, risk acceptance, resource constraints, etc.) and approval in the System Security Plan (SSP).

- An alternate storage site will be identified:
 - The site will be in a secure, geographically different location than the primary site.
 - Agreements will be initiated to permit the use of the site.
- An alternate processing site will be identified:
 - The site will be a in a geographically different location than the primary site.
 - Agreements will be initiated to permit the resumption of information system operations for business and mission critical systems within 48 hours.
 - Equipment and supplies necessary for resumption of services will be located at the alternate processing site or contracts in place to support delivery to the site.
 - Potential accessibility issues will be identified and explicit mitigating actions will be outlined.
 - Agreements with the alternate site will contain a priority-of-service provision in accordance with PSA availability requirements.
- Alternate telecommunication services will be identified:
 - Agreements will be initiated to allow for resumption of telecommunications service within 48 hours.
 - Alternate telecommunication services will not share a single point of failure with primary services.
 - The alternate telecommunications services agreement will contain a priority of service provisions in accordance with PSA availability requirements.

- All business and mission critical systems information will be backed up:
 - There will be daily (i.e. Monday through Thursday) incremental backups of the system information to tape.
 - There will be a weekly (Friday) full system backup to tape.
 - There will be an archival backup of the system to tape once a month.
 - Tapes will be used on a four-week backup cycle, and will be rotated at the end of eight weeks.
 - All backup information will be tested once a week to ensure media reliability and information integrity.
 - Backup information will be stored at an appropriately secured location.
- A mechanism will be employed to allow the system to be recovered and reconstituted to its original state including:
 - Reinstallation of all system patches.
 - Resetting all system parameters.
 - Reestablishing all configuration settings.
 - Restoring the most recent backup information.
 - Running a full test on the system.
- PSA will develop and implement a contingency plan that includes operational procedures for disaster recovery and continuity of support. The plan will delineate:
 - Roles and responsibilities, including contact information.
 - Activities associated with restoring the system after a disruption or failure.
- All personnel with contingency planning roles and responsibilities will participate in annual training in the use and application of the PSA Continuity of Support/Disaster Recovery Plan (COS/DR Plan).
- The effectiveness of all recovery and reconstitution procedures in the plan and the readiness of PSA personnel to carry out these procedures will be tested annually.
- The Director PSA Office of Information Technology will review test results, and corrective measures will be instituted.
- The COS/DR Plan will be reviewed, revised and redistributed annually in order to address any system or organizational changes, as well as any problems that have been encountered in the implementation, execution or testing of the plan.

- The COS/DR Plan and any subsequent updates will be coordinated with related plans (e.g., CSOSA/PSA Continuity of Operations Plan, PSA Incident Response Plan, PSA Configuration Management Plan, etc.).
- The COS/DR Plan will be reviewed and approved by the Director PSA Office of Information Technology, and multiple copies of the plan will be distributed to key contingency personnel.

E. Roles and Responsibilities

A current list of roles and responsibilities will be maintained delineating responsibilities for executing, managing, monitoring and enforcing the procedures in this management instruction.

Table I –Roles and Responsibilities

Role	CP Responsibilities
<ul style="list-style-type: none"> • Configuration Manager • Inventory Manager 	<ul style="list-style-type: none"> • Maintain up-to-date configuration of critical hardware and software.
Media Protection Manager	<ul style="list-style-type: none"> • Ensure that required operating systems are backed up to tape and stored at the off-site facility. • Maintain updated vendor manuals for critical hardware and software. • Maintain network recovery procedures and configurations.
Disaster Recovery/Contingency Planning Services Manager	<ul style="list-style-type: none"> • Maintains the disaster recovery plan. • Distributes disaster recovery plan to all parties. • Defines and institutes the emergency operating procedures. • Coordinates continuity planning with the Office of Operations, the Office of Finance and Administration, the Forensic Toxicology Drug Testing Laboratory and the Office of Human Resources and Strategic Planning, Analysis & Evaluation. • Assigns DR/CP roles and responsibilities. • Periodically reviews and tests backup and restoration plans and procedures and system recovery and restoration timelines. • Ensures compliance with the CP Management Instruction.
System Manager	<ul style="list-style-type: none"> • Maintains operations manuals for each user. • Maintains updated vendor manuals for critical hardware and software.
PSA Data Center Manager	<ul style="list-style-type: none"> • In event of a disaster, receives reports from SRT team, declares a disaster, activates alternate processing site, manages primary/alternate site recovery. • Maintain updated vendor manuals for critical hardware and software.
Office of Human Resources & Strategic Planning, Analysis and Evaluation	<ul style="list-style-type: none"> • Activate Emergency and Evacuation Plan. • Notification of family of injured and deceased personnel; handle media and public relations once authorized. • Interface with CSOSA for available personnel.
Office of Finance & Administration	<ul style="list-style-type: none"> • Monitor all disaster related expenses and labor charges. • Procure construction and maintenance services, supplies, and equipment.
Vendors	<ul style="list-style-type: none"> • Replace hardware and restore operations at damaged site.

Role	CP Responsibilities
PSA Office of Facilities	<ul style="list-style-type: none"> • Determine the extent of damage. • Determine what equipment can be salvaged and what needs to be replaced. • Coordinate public relations activities with the PSA Director. • Coordinate repair or reconstruction activities. • Contact facility contractors. • Coordinate activities with PSA Procurement. • Coordinate deliveries to and from the damaged site. • Coordinate with the CSOSA Director of Security to determine if damage has any physical security ramifications.
Technical Personnel	<ul style="list-style-type: none"> • Restore the necessary operating system software. • Provide technical support to the application, operations, and data communications team.
Contingency Planning Committee	<ul style="list-style-type: none"> • Develop, document and test disaster recovery plan. • Coordinate training activities within individual functional areas.

F. Authorities and References

- PSA Policy Statement # 5500, *Global Information Technology Security Policy for PSA Business and Mission Critical Systems*
- PSA Policy Statement #5506, *Contingency Planning Policy for Business and Mission Critical Systems*
- PSA Policy Statement #5510, *Media Protection Policy for PSA Business and Mission Critical Systems*
- PSA Management Instruction, PS #5560, *Media Protection for PSA Business and Mission Critical Systems*
- Federal Information Security Management Act of 2002 (FISMA)
- OMB Circular A130, Appendix III
- Recommended Security Controls for Federal Information Systems (NIST SP 800-53)
- Risk Management Guide For Information Technology Systems (NIST SP 800-30)
- An Introduction To Computer Security – The NIST Handbook (NIST SP 800-12)
- Guide For Developing Security Plans For Information Technology Systems (NIST 800-18)
- Contingency Planning Guide for Information Technology Systems (NIST SP 800-34)

G. Attachments

- Security Control Reference Guide