



The National Science Foundation Office of Polar Programs United States Antarctic Program

Information Resource Management Directive 5000.13 USAP Contingency & Disaster Recovery Program

Organizational Function	Information Resource Management	Policy Number	5000.13
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Updated	24 April 2007
Subject	Contingency & Disaster Recovery	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Antarctic Infrastructure & Logistics	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.usap.gov		

1. PURPOSE

This directive establishes the program to develop and maintain a Contingency & Disaster Recovery (C&DR) Program for the National Science Foundation (NSF) Office of Polar Programs (OPP) United States Antarctic Program (USAP). This program includes contingency and disaster recovery planning for information systems supporting USAP science and operations activities. The program shall create plans for contingency and disaster response. These plans will be tested periodically to ensure they reflect current operating conditions and address current threats.

2. BACKGROUND

Federal information technology regulations presented in OMB Circular A-130 and supporting legislation require USAP information systems to have plans for contingencies and disaster recovery, to determine the proper actions to accomplish in the event of a disaster. An effective contingency and disaster recovery program ensures science and operations activities continue at locations not affected by the disaster while recovery proceeds at the affected site.

3. GUIDING PRINCIPLES

- The USAP Contingency & Disaster Recovery Program shall be developed following existing NSF and NIST guidelines.
- The USAP Contingency & Disaster Recovery Program will require the involvement of all USAP participants to ensure an effective response to contingencies and disasters.
- The USAP Contingency & Disaster Recovery Program must incorporate the physical and logistical limitations of the USAP operating locations.
- The USAP Contingency & Disaster Recovery Program will be aligned with the OPP Emergency Response Program

4. POLICY

The USAP shall establish a program to develop, maintain, and evaluate plans to appropriately respond to a wide range of contingencies and disasters that may occur at all of the USAP operating locations. The plans shall describe the actions to be taken before, during and after events that disrupt critical information system operations.

4.1 Operational Definitions

4.1.1 Contingency Planning

A coordinated strategy involving plans, procedures and technical measures that enable the recovery of information systems, operations and data after disruption. Such measures may necessitate relocating IT systems and operations to an alternate location, using alternate equipment to recover IT functions, or performing IT functions using manual methods.

4.1.2 Contingency Plan

The contingency plan is a set of procedures created to restore operations to normal conditions. A contingency plan must involve procedures for preparation, testing, and updating the actions required to protect critical processes from the effects of major system and network failures. An IT contingency plan must also identify critical and sensitive activities and their supporting information systems.

4.2 Contingency Response

4.2.1 Station Contingency Plan

Each USAP operating location shall have an Information Systems Contingency Plan that addresses contingencies and potential disasters for each Major Application and General Support System in use at that location. The plan will be integrated with the larger station emergency response plan for that location, and will be consistent with OPP guidelines for emergency response within the USAP. The plan will be based on a risk assessment of conditions at the location. The station manager will ensure that an Information Systems Contingency Plan is created for their location. The station Information Systems Contingency Plan will be integrated with other station disaster response and recovery

plans, and with the station Information Security Incident Response Capability (see 5000.12, USAP Incident Response Capability).

4.2.2 System Contingency Plans

Each Major Application and General Support System at each operating location will have an associated contingency and disaster response plan. The system owner will ensure that an Information Systems Contingency Plan is created for their system, following NSF and NIST guidelines. Where a system exists at multiple locations, the system owner will create a basic plan, and local IT managers will augment the plan with their site-specific responses.

4.2.3 Information Systems Contingency Response Coordinator

The station IT manager serves as the coordinator for response to contingencies and disasters affecting station information systems. Where the contingency or disaster affects more than just station information systems, the station IT manager integrates their activities as directed by the station manager and station disaster response procedures.

4.2.4 Station Risk Assessment

The USAP ISM and station management will prepare a risk assessment for each station that considers the station's unique features and limitations. The USAP ISM, in consultation with the station IT managers, will establish a list of potential contingency and disaster situations for each station. The list will evaluate the probability of occurrence and the severity of occurrence, and will be used to assist in the risk management process for that station. The risk assessment will follow NSF and NIST guidelines for risk assessments. The risk assessment will address threats and contingencies specific to the station, in the areas of natural disaster, environmental threats, and human –originated threats, either accidental or malicious. The risk assessment will be reviewed annually according to NSF guidelines.

4.2.5 Prioritization of Recovery

The USAP Technology Manager will prioritize activities and their supporting information systems at each location to determine the criticality of each system and the order of restoration during a contingency or disaster situation. The USAP Information Security Manager, with support from the Prime Contractor, will establish and maintain a list of mission critical operations systems, and their components, for each site. This list will be part of the station contingency plan. Prioritization will address the information's categorization, as identified in USAP Information Security Policy 5000.3, Information Categorization.

4.2.6 Contingency Response Resource

Each station manager will establish a contingency response team and staff it according to the station's needs. Contingency Team members may not necessarily be the same resources as assigned to the Incident Response team. Each station IT manager will maintain a checklist for each team position that assigns responsibility for the tasks each team member will be expected to complete during a contingency or disaster. The station

IT manager will train personnel assigned to the Contingency Team, as well as those responsible for specific systems.

4.2.7 Contingency Plan Testing

The USAP Prime Contractor will test the contingency plan on a quarterly basis. The quarterly testing will be organized to test all plan elements and all related operations procedures at least once annually. Where possible, the testing will be integrated with the testing of other site response plans. After each test of a plan element, the Prime Contractor will forward an After Action report to the USAP Information Security Manager. The report will include lessons learned from the testing, deficiencies noted during the testing, and a plan to remedy those deficiencies. The USAP Information Security Manager will ensure funding is included in the annual budget to support the Contingency Testing program. The USAP ISM will include a proposed test program in the annual update of the USAP Information Security Plan.

4.3 Information Systems Recovery

4.3.1 Alternate Operating Capability

Each USAP operating location will have a designated alternate location for establishing temporary control of information resources during a contingency or disaster. Normally such a site will be geographically removed from the immediate disaster location. For the Antarctic research stations, the alternate location will be isolated from the primary operations to the extent possible.

4.3.2 System Redundancy

The Prime Contractor, as manager of the USAP infrastructure, will determine and implement a cost-effective means for providing redundant operations at all stations. This includes maintaining suitable spares or replacement equipment for all mission critical systems.

4.3.3 Information Back-Up and Recovery

The Prime Contractor shall establish operations procedures for creating, maintaining, and storing information backup media to support contingency response and disaster recovery activities at each operating location. Each station's procedures for data backup will include a schedule for daily, weekly, and monthly backups. Each station shall establish media control procedures that include steps for the preparation of media for reuse, or destruction. Using the Recovery Prioritization list, each station will prepare an information backup plan that ensures information is saved according to its priority for recovery.

4.3.4 Information Retention and Archive

Backup media should be retained on station for operational use up to one year after its creation. One year after its creation, backup media will be reviewed, and if appropriate, archived to comply with guidance from the National Archives and Records Administration. Every six months, or at the end of each operational season, the station IT

managers will review all backup media to identify archival data. Archival data will be removed to the program headquarters facility for disposition and storage. Backup media that has passed the one-year retention point and is not scheduled for archiving will be prepared for reuse, or destroyed if appropriate. Station IT managers may forward their backup media to the program headquarters for storage if space limitations preclude on-site storage.

4.3.5 Offsite Storage Of Backup Material

Where possible, backup media will be stored at a suitable off-site location. For locations where off-site storage is not practicable, such as the Antarctic research stations and vessels, the station manager will designate an appropriate facility to serve as the off-site storage of backup media. A suitable facility is one within reasonable distance of the main station, but not likely to be immediately threatened by the contingency or disaster. The nature of vessel operations precludes the use of an offsite or removed facility. Vessel backup material will be stored in an appropriate location aboard the ship, but removed from the main IT area.

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program*.

6. RESPONSIBILITIES

6.1 NSF Director of Polar Programs

The NSF Director of Polar Programs ensures a comprehensive cost-effective security program is in place to protect NSF USAP information systems. After recovery from a contingency or disaster is complete, the Director of Polar Programs or their designated representative, approves the return to normal system operations.

6.2 NSF Technology Development Manager

The NSF OPP Technology Development Manager coordinates Information Systems Contingency and Disaster Response with other USAP participant organizations, and with other NSF staff elements.

6.3 USAP Information Security Manager

The USAP Information Security Manager manages the Information Systems Contingency & Disaster Response program. The ISM will establish processes and procedures for enterprise contingency response and recovery. The ISM supports the development of procedures by each USAP organization, and maintains awareness of the external threat environment.

6.4 USAP Information Systems Managers and Administrators

The information system managers and administrators have a significant role in the successful response to and recovery from information security contingencies and disasters. Depending on the circumstances, the system managers and administrators will usually provide the technical expertise at the core of the response.

7. POLICY IMPLEMENTATION

7.1 Guiding Standards

The USAP Contingency & Disaster Response program will be based on existing federal and NSF directives.

7.2 Publication of Contingency Procedures.

Each USAP participant organization will establish internal procedures for implementing this policy, and provide copies to the USAP Information Security Manager. The USAP procedures will implement NSF Manual 7 and appropriate federal regulations. The participant organizations will coordinate their procedures with the OPP Emergency Response Working Group to ensure compliance with OPP Emergency Response Guidelines.

7.3 Policy Review

The USAP Information Security Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP.

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director