



The National Science Foundation Polar Programs United States Antarctic Program

Media Protection Policy

5000.22

Organizational Function	Information Resource Management	Policy Number	5000.22
		Issue Date	06/27/2014
Policy Category	Information Security Policies	Effective Date	06/27/2014
		Review On	06/27/2016
Subject	Media Protection	Authorized By	Mr. Brian Stone Section Head, NSF/PLR/AIL
Office of Primary Responsibility	National Science Foundation Geosciences Directorate Division of Polar Programs Antarctic Infrastructure and Logistics	Responsible Official	Primary Responsibility: Mr. Patrick D. Smith Technology Development Manager Security Responsibility: Ms. Desari Mattox USAP Information Security Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	http://www.nsf.gov/div/index.jsp?div=PLR
Distribution	USAP-Wide	Status	Final
Online Publication	http://www.usap.gov/technology/contentHandler.cfm?id=1563		

Document Release History

Release Number	Release Date	Description of Changes	Changes Made By
0.1		Initial Creation	Matthew Rogers -BAH
1.0	06/13/2014	Updates throughout	USAP ISM

Table of Contents

1	PURPOSE	4
2	BACKGROUND	4
3	GUIDING PRINCIPLES	4
4	POLICY	4
5	ROLES AND RESPONSIBILITIES	5
5.1	Technology Development Manager, Antarctic Infrastructure & Logistics (AIL)	5
5.2	USAP Information Security Manager (ISM)	5
5.3	Supporting Organizations	5
5.4	Tenant Organizations	5
6	SCOPE AND COMPLIANCE	5
7	POLICY IMPLEMENTATION	5
7.1	Implementation	5
7.2	Policy Review	5
8	AUTHORITY	6

THIS PAGE INTENTIONALLY LEFT BLANK

1 PURPOSE

This directive establishes the policy for media protection as it relates to information systems supporting the National Science Foundation (NSF) United States Antarctic Program (USAP) managed by the NSF Division of Polar Programs (PLR).

2 BACKGROUND

Federal law and Office of Management and Budget (OMB) directives require the establishment of a media protection policy to protect USAP information and information systems.

3 GUIDING PRINCIPLES

In developing methods and processes for protecting media, the program shall follow these guiding principles:

- The USAP Media Protection Program shall be developed in compliance with National Institute of Standards & Technology (NIST) guidelines and NSF/PLR directives.
- Media protection secures data through the access, marking, storage, transport, sanitization and use of media storage devices.
- Media containing personally identifiable information (PII) and sensitive information (SI) shall be subject to additional protections
- All media (digital and non-digital) owned and/or controlled by USAP shall be protected throughout the media lifecycle.

4 POLICY

It is USAP policy to protect the confidentiality, integrity and availability of information systems, digital media (e.g., diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks) and non-digital media (e.g., paper and microfilm).

System operators, managers, maintainers and providers of USAP information & communication systems shall:

- Restrict access to USAP media, digital and non-digital, to authorized personnel.
- Label USAP media following the USAP labeling requirements.
- Physically control and secure media until the media is destroyed or sanitized.
- Only allow authorized personnel to transport digital and non-digital media outside of USAP controlled areas.
- Protect all media containing PII and SI during use, storage, transport, sanitization and disposal.
- Encrypt all types of removable media used to store PII/SI.
- All information system media shall be sanitized prior to disposal or release for reuse.
- Document media protection procedures.

5 ROLES AND RESPONSIBILITIES

The following roles have specific responsibilities pertaining to media protection management. The sections below describe only the responsibilities for these roles as they relate to media protection management. Refer to USAP Information Security Policy 5000.01, *The USAP Information Security Program*, for the full description of the responsibilities for these roles.

5.1 Technology Development Manager, Antarctic Infrastructure & Logistics (AIL)

The AIL Technology Development Manager is the responsible official of the USAP media protection management program

5.2 USAP Information Security Manager (ISM)

The USAP Information Security Manager (ISM) oversees the media protection management program. The ISM coordinates the development and implementation of the media protection program with Supporting Organizations, System managers, and administrators of USAP information systems to ensure that digital and non-digital media are protected throughout the media lifecycle.

5.3 Supporting Organizations

Supporting organizations are responsible for management of the media protection processes and implementation of security controls. Also ensure that media protection is in alignment with guidance from NSF/PLR. Personnel shall provide USAP participants with support and guidance in media protection.

5.4 Tenant Organizations

Tenant organizations with systems interconnected to the USAP enterprise network are responsible for media protection in accordance with this policy.

6 SCOPE AND COMPLIANCE

This policy applies to supporting organizations and tenant organizations within the USAP operating environment or connected to the USAP network. Compliance with this policy implementation is indicated in OMB M-06-16 – *Protection of Sensitive Agency Information*, National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and USAP Information Security Policy 5000.01, *The USAP Information Security Program*.

7 POLICY IMPLEMENTATION

7.1 Implementation

Each USAP supporting organization shall develop appropriate processes, and procedures to implement the USAP Media Protection Program. Supporting organizations shall publish procedures as appropriate to implement this program and comply with this policy.

7.2 Policy Review

This policy is reviewed in conjunction with major changes to the USAP information infrastructure, or every two years.

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 Guidance.

Brian Stone
Section Head, NSF/GEO/PLR/AIL