



**DRYDEN
POLICY
DIRECTIVE**

Directive: DPD-2800.2
Effective Date: October 22, 2004
Expiration Date: October 22, 2009

This document is uncontrolled when printed.
Before use, check the Master List to verify that this is the current version.
Compliance is mandatory.

RESPONSIBLE OFFICE: V/Chief Information Officer

SUBJECT: Managing Information Technology (IT)

1. POLICY

a. Computer systems, networks, data repositories, and other IT equipment are critical resources used to support the transfer of information and vital data Agency-wide. Protecting integrity and interoperability, and eliminating IT vulnerabilities Center-wide shall be a priority of all computer users and System/Network Administrators. Computer systems, networks, data repositories, and other IT equipment will be configured consistent with all requirements established by the Chief Information Officer (CIO) at Dryden.

b. In order to affect a broad and cost-effective IT infrastructure, standard interfaces and products will be used for interoperability and to protect systems against unauthorized access and disruption of service. All products installed on Dryden-controlled equipment will utilize CIO standards for software and hardware interoperability.

c. Form DFRC 316, Chief Information Waiver Request, must be submitted for approval when a system or network can not be configured to standards.

d. Non-compliance with this policy resulting in an IT Security incident as a result of negligence, misuse, or intentional lack of following established requirements may result in lower employee performance ratings, lower contract performance ratings, removal of equipment from the network, or other management action as appropriate.

2. SCOPE AND APPLICABILITY

This policy applies to the all installed devices on the Dryden computer network and is applicable to all Dryden employees and contractors who, within the scope of their contract, utilize or maintain computer equipment, networks, data repositories, or other IT equipment.

3. AUTHORITY

a. Title III of Public Law 107-347, E-Government Act of 2002, Federal Information Security Management Act (FISMA)

b. Executive Order No. 13011, Federal Information Technology, July 16, 1996

c. OMB Circular No. A-130, Management of Federal Information Resources

d. Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection, December 17, 2003

4. REFERENCES

- a. Chief Information Officer Website,
- b. NPR 2810.1, Security of Information Technology, August 26, 1999
- c. NASA-STD-2804H, Minimum Interoperability Software Suite
- d. NASA-STD-2805H, Minimum Hardware Configurations

5. RESPONSIBILITY

The Chief Information Officer will:

- a. Establish and maintain standard configuration requirements and procedures for all computers, networks, data repositories, and other IT equipment to ensure the integrity and interoperability of Dryden systems and data.
- b. Reasonably assure compliance with this policy through risk management or take action to correct discrepancies using appropriate disciplinary channels.
- c. Work with Contracting Officers to ensure that contract language addresses system and network administrator responsibilities.
- d. Work with supervisors to ensure Organizational Computer Security Official, System Administrator, and Network Administrator responsibilities are outlined in employee performance plans.

The System and Network Administrators will:

- a. Maintain a valid and current NASA Dryden Computer System Administrator Certification in their respective areas of coverage.
- b. Actively participate in System Administrator meetings and training provided.
- c. Ensure vulnerabilities and system upgrades are addressed when required or a waiver has been approved for the non-compliance prior to the compliance date.
- d. Meet the outlined IT responsibilities in their performance plan or contract agreement.

The Computer Users will:

- a. Be knowledgeable of and comply with IT and IT Security regulations and established policies and procedures.
- b. Report questionable computer activity to the IT Security Manager.
- c. Complete all required IT and IT Security training.

The IT Security Manager will:

- a. Ensure all required administrator and IT Security training is completed.
- b. Actively lead and participate in System Administrator meetings.
- c. Ensure all IT systems have an assigned Certified Administrator.
- d. Ensure vulnerability scan reports are completed in a timely and efficient manner.

The Organizational Computer Security Officials will:

- a. Serve as the critical communication link to and from their organizations for all IT Security matters.
- b. Actively participate in System Administrator meetings.
- c. Maintain, for their organizations, an accurate list of all IT resources with corresponding users and system administrators.
- d. Meet the outlined IT responsibilities in their performance plan

6. DELEGATION OF AUTHORITY

None

7. MEASUREMENTS

Network Engineering and IT Security will perform monthly system audits. Determination of the effectiveness of this policy will be based on the number of system configurations that fail to comply with the configuration requirements established by the CIO.

8. CANCELLATION

None

/S/ Kevin L. Petersen or Delegated Official

ENCLOSURES:

None

DISTRIBUTION:

- IDMS
- System Administrator Meetings
- Staff Meetings
- CIO Home Page
- DM3

Document History Log

This page is for informational purposes and does not have to be retained with the document.

Status Change	Document Revision	Effective Date	Page	Description of Change
Baseline		10-25-04		
Admin. Change		11-18-04	1	<ul style="list-style-type: none"> • Added "Compliance is mandatory." to first page. • Corrected typographical, grammatical, and some format errors.