



**DRYDEN
POLICY
DIRECTIVE**

Directive: DPD-2810.1-001 Baseline-3
Effective Date: May 1, 2009
Expiration Date: May 1, 2014

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

SUBJECT: Network Monitoring

RESPONSIBLE OFFICE: MI/Chief Information Officer

1. POLICY

a. Dryden shall continuously monitor electronic communications to ensure the proper use of IT resources by its workforce, to gauge the performance and availability of its networks and services, and to secure its data and information systems from hostile intrusions, misuse, and other threats. The function of monitoring Dryden networks and services shall be limited to the Office of the Chief Information Officer (OCIO) Network and Information Technology (IT) Security personnel, and shall be conducted as follows:

(1) The OCIO network personnel shall be responsible for routine monitoring of all Dryden networks and services to ensure availability and performance including remote sites.

(2) The OCIO IT security personnel shall be responsible for detecting intrusions, monitoring for illegal software and malicious code, and monitoring for unauthorized network devices, services, ports, or protocols. If suspicious traffic, criminal or noncriminal, is discovered during routine monitoring, incident response policies shall be followed.

b. The monitoring (encrypted or unencrypted) of inbound or outbound traffic on the Dryden network shall be based on risk management principles, with a higher concentration on those assets deemed most critical to NASA.

c. Dryden's IT resources are the property of the U.S. Government; therefore, Dryden shall monitor all aspects of computer usage at any time. Monitoring includes the following activities.

(1) Monitoring can include ports, IP addresses, protocols, and content. Monitoring shall be performed either by automated means, such as intrusion detection systems and flow-based content monitors, or by manual inspection of the contents of captured network data or log data. A diverse and dynamic range of computer tools are used and tested to perform monitoring activities.

Before use, check the Master List to verify that this is the current version.

(2) All Network Monitoring and Intrusion Detection Logs shall be centrally managed. Access to the monitoring systems and central log system shall be restricted to authorized OCIO network and IT security personnel. All logs and information collected by network monitoring tools shall be maintained and preserved in accordance with NPR 1441.1, NASA Records Retention Schedule, and shall be properly safeguarded and not released beyond the OCIO network and IT security personnel unless approved by the Dryden CIO.

(3) All requests for network monitoring shall be coordinated with the Information Technology Security Manager (ITSM).

2. SCOPE AND APPLICABILITY

a. **Scope:** This policy applies to all IT resources and services connected to the DFRC network.

b. **Applicability:** This policy applies to Dryden Flight Research Center civil servants and on-site support contractors, grant recipients, and other partners to the extent specified in their contracts or agreements.

3. AUTHORITY

a. NPR 2810.1, Security of Information Technology

4. REFERENCES

a. NPD 1441.1, NASA Records Retention Schedule

b. NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology

5. RESPONSIBILITY

a. The Dryden CIO is responsible for maintaining responsibility and accountability for Center-specific implementation of the Dryden network monitoring program; informing the Center Director, as appropriate, of monitoring activity and findings; and reviewing and approving testing agreements and protocols for evaluations of monitoring technology in the Center network environment.

b. The Dryden ITSM is responsible for reviewing suspicious activities identified during routine monitoring to determine the course of action; notifying law enforcement of suspected criminal activities identified during monitoring; reviewing and approving requests for targeted monitoring from authorized NASA managers and law enforcement officials; maintaining documentation of all targeted monitoring activities involving the Center, including law enforcement or other requests for targeted monitoring and

receipts for targeted monitoring records; and informing NASA Dryden managers and the Center CIO, as appropriate, of the results of targeted monitoring.

c. The OCIO Network and IT Security Personnel are responsible for conducting monitoring as directed under the NASA IT security monitoring program; maintaining audit logs of all routine monitoring activities, as well as identified suspicious activities recommended for further targeted monitoring; reporting to the Center ITSM or other appropriate management chain any suspicious activity identified during routine monitoring; providing technical support and monitoring services for approved targeted monitoring activities; informing the Center ITSM on the progress and results of targeted monitoring; providing records of approved targeted monitoring to the requestor; and properly safeguarding all data collected from monitoring.

6. DELEGATION OF AUTHORITY

None

7. MEASUREMENTS

None

8. CANCELLATION

None

/S/ David McBride or Delegated Official

ATTACHMENTS

None

DISTRIBUTION

Approved for release via the DFRC Document Library; public distribution is unlimited.

Document History Log**Review Date:**

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		05/01/09		
Admin Change	Baseline-1	07/23/09	All	<ul style="list-style-type: none"> Added serial number to document name. Name changed from DPD-2810.1 to DPD-2810.1-001. The content did not change.
Admin Change	Baseline-2	12/10/09	2	<ul style="list-style-type: none"> Replaced reference to cancelled document DPD-2800.1-001, Personal Use of Government Office Equipment Including Information Technology, with reference to NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology
Admin Change	Baseline-3	07/13/10	All	<ul style="list-style-type: none"> Changed Code V to Code MI Changed formatting to comply with Agency standards

Before use, check the Master List to verify that this is the current version.