Information Technology Requirement

NASA Rules and Consequences Policy Relative to Safeguarding Personally Identifiable Information (PII)

ITS-NITR-1382-2
Version Date: 20080128
Effective Date: 20080130
Expiration Date: 20120810
Responsible Office: Office of the Chief Information Officer

Revision Record

ITEM NO.	REVISION	DESCRIPTION	DATE
1	V.1.0	Initial	January 28, 2008

NASA Rules and Consequences Policy Relative to Safeguarding Personally Identifiable Information (PII)

1. Purpose

This NASA IT Requirement (NITR) document sets forth NASA rules of behavior for maintaining and protecting personally identifiable information (PII) as defined in NPR 1382.1, as well as the consequences and corrective actions available for failure to follow these rules. All NASA employees have a duty to protect from loss or misuse information about an individual that is maintained by the Agency. PII includes Social Security Numbers (SSNs), medical and financial information about individuals, home addresses, and home telephone numbers.

2. Scope

2.1. These requirements apply to the handling and protection of all PII collected and/or maintained by, or on behalf of, NASA in the conduct of Agency business.

3. Applicability

3.1. This NITR is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers.

3.2 This NITR applies to the NASA Jet Propulsion Laboratory (JPL), other contractors, grant recipients, and parties to agreements, to the extent that they collect and/or maintain PII, or develop and administer systems containing PII, on behalf of NASA.

4. Authority

a. 42 U.S.C. § 2473(c) (1), The National Aeronautics and Space Act of 1958, as amended

b. 5 U.S.C. § 552a, The Privacy Act of 1974, as amended.

c. 44 U.S.C. §§ 3541 et seq., Federal Information Security Management Act of 2002

5. Requirements

5.1 **Rules of Behavior**

5.1.1 All NASA personnel shall:

a. Protect all Personally Identifiable Information (PII) in their custody from unauthorized disclosure, modification or destruction so that the security and confidentiality of the information is preserved.

b. Encrypt all PII they transmit and all PII that they download to mobile computers/devices.

c. Report to the Center Privacy Act Manager (PAM) or IT Security Manager (ITSM) any unauthorized disclosures of PII in accordance with Agency IT Security incident reporting procedures.

5.1.2 NASA system owner for each system containing PII shall:

a. Implement and maintain technical and administrative security controls for systems categorized at a minimum of Moderate per FIPS 199.

b. Ensure that all personnel who have access to the data or who develop or supervise procedures for handling PII are trained and are compliant with policies and procedures for safeguarding PII collected and maintained at NASA.

c. Limit the maintenance of files on individuals, which are retrievable by name or other personal identifier, to only instances for which a Privacy Act system of records notice has been published in the Federal Register in accordance with NPR 1382.1.

5.2 **Consequences and Penalties**

5.2.1 The consequences of violating the above rules of behavior are defined in the Privacy Act of 1974 as amended. The consequences available under the Privacy Act range from administrative to criminal. Supporting guidance on the consequences for managers and supervisors is provided in the NASA Desk Guide, Table of Disciplinary Offenses and Penalties of March 2006.

5.2.2 Any official who willfully maintains a Privacy Act system of records without meeting the publication requirements is subject to possible criminal penalties or administrative sanctions, or both.

5.2.3. Any person who knowingly and willfully requests or obtains any Privacy Act record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

5.2.4. Any employee with possession of, or access to PII who willfully discloses the material in any manner to any person or agency not entitled to receive it, may be guilty of a misdemeanor and fined not more than $5,000.

5.2.5 Employees may be subject to written reprimand, suspension, or removal under the following situations:

a. Knowingly failing to implement and maintain information security controls required by NPR 1382.1 for the protection of PII regardless of whether such action results in the loss of control or unauthorized disclosure of PII.

b. Failing to report any known or suspected loss of control over or unauthorized disclosure of PII.

c. For managers, failing to adequately instruct, train, or supervise employees in their responsibilities.

6. References

a. OMB M-07-16, Safeguarding against and Responding to the Breach of Personally Identifiable Information

b. NASA NPD 1382.17G, NASA Privacy Policy

c. NASA NPR 1382.1, NASA Privacy Procedural Requirements

d. NASA NPR 2810.1A, Security of Information Technology

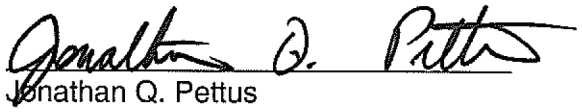
e. NASA NPR 1600.1, NASA Security Program Procedural Requirements

f. Executive Order 13402, May 10, 2006, President's Identity Theft Task Force and the Task Force's report: Combating Identity Theft – A Strategic Plan, April 2007

g. OMB Circular A-130, Management of Federal Information Resources

h. OMB M-06-16, Protection of Sensitive Agency Information

i. NASA Desk Guide for Table of Disciplinary Offenses and Penalties, March 2006



Jonathan Q. Pettus
Chief Information Officer

1-30-08
Date