GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO P 2180.1

GSA POLICY AND PROCEDURE

SUBJECT: GSA Rules of Behavior for Handling Personally Identifiable Information (PII)

1. Purpose. This directive provides GSA's policy on how to properly handle PII and the consequences and corrective actions that will be taken when a breach has occurred.

2. Background. This satisfies the requirement to develop and implement policy outlining rules of behavior and consequences included in the Office of Management and Budget Memo OMB Memorandum M-07-16 (May 22, 2007).

3. Applicability. This order applies to all GSA officials, employees, contractors, and to those who manage information technology (IT) systems that contain PII. It applies to the Office of Inspector General (OIG), only if it is consistent with the OIG's independent authority under the IG Act and it does not conflict with other OIG policies or mission. Contractors are not subject to the provisions of internal GSA discipline.

4. Cancellation. HCO 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII) dated August 7, 2009, is cancelled.

5. Responsibilities. The complete list of roles and responsibilities can be found in GSA CIO P 2100.1I Information Technology (IT) Security Policy. A link to the FISMA System Inventory Points of Contact can be found on GSA Insite.

6. Signature.

/S/_____
SONNY HASHMI
Senior Agency Official for Privacy
Office of GSA IT

October 29, 2014
Date

TABLE OF CONTENTS

GSA Rules of Behavior for Handling Personally Identifiable Information (PII)

1. Definitions.

Personally Identifiable Information (PII) – information about a person that contains some unique identifier, including but not limited to name or Social Security Number, from which the identity of the person can be determined. OMB Memorandum M-10-23 (June 25, 2010), updated the term "PII": "The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual."

Data Breach – Includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic. In the case of this policy, the term "breach" and "incident" mean the same.

2. Protecting PII.

The GSA Information Technology (IT) Security Policy lists measures that should be taken to protect PII. Chapter 4, Policy of Operational Controls, Section 23, Personally Identifiable Information, has security requirements for the protection of PII. Please use the link provided to access the most current version of this policy.

3. Privacy and Security Awareness training and education.

   a. All employees and contractors must complete the "IT Security Awareness and Privacy Training 101" training within 30 days of employment.

   b. All GSA employees and contractors must complete the "IT Security Awareness and Privacy 101" training annually.

   c. All employees and contractors who have information security responsibilities as defined by 5 CFR 930.301 and CIO 2100.3B Mandatory IT Security Training Policy must complete specialized IT security training as defined in said policy.

   d. All employees and contractors who have significant privacy information responsibilities must complete specialized Privacy Training 201. This includes employees and contractors who work with PII as part of their work duties. (i.e.; Human Resource staff, Finance staff, or managers/supervisors)

e. All GSA employees and contractors, who work with PII or have access to other people's information, must complete Privacy Training 201.

f. Failure to comply with annual awareness and specialized training requirements will result in termination of email privileges.

4. Information data breach.

A data breach is when PII is or potentially viewed, or accessed by anyone who is not the individual or someone authorized to have access to this information as part of his/her official duties. In accordance with GSA IT Security Procedural Guide: Handling IT Security Incidents, a "security incident" is "[a] set of events that have been examined and determined to indicate a violation of security policy or an adverse effect on the security status of one or more systems within the enterprise." When it has been determined that PII has been compromised, refer to HCO 9297.2B GSA Information Breach Notification Policy.

5. Corrective action and consequences.

a. Employees.

(1) Penalties for non-compliance. All users who do not comply with the IT General Rules of Behavior may incur disciplinary action and/or criminal action per CIO 2104.1A GSA IT Rules of Behavior (para. 6).

(2) Compliance and deviations. Compliance is mandatory. CIO P 2100.1I IT Security Policy requires all GSA Services, Staff Offices, Regions, Federal employees, and authorized users of GSA's IT resources to comply with the security requirements outlined in the policy. The policy must be properly implemented, enforced, and followed to effectively protect GSA's IT resources and PII. Appropriate disciplinary action may be taken in a timely manner in situations where individuals and/or systems are found non-compliant. Violations of GSA IT Security Policy may result in penalties under criminal and civil statutes and laws. All deviations from the GSA IT Security Policy must be approved by the appropriate Authorizing Official with a copy of the approval forwarded to the Chief Information Security Officer (CISO) in the Office of GSA IT (formerly known as the Senior Agency Information Security Officer or SAISO).

b. Contractors.

(1) When GSA contracts are for the design, operation, maintenance, or use of systems containing information covered by the Privacy Act, the contractor and its employees are considered employees of GSA for purposes of safeguarding the information and are subject to the same requirements for safeguarding the information as Federal employees. (5 U.S.C. 552a(m)).

(2) Contractors and their employees are subject to criminal sanctions under the Privacy Act for any violation that may occur due to oversight or negligence.

6. Security violation.

All breach incidents that involve PII must be reported to the CISO, as stated in CIO P 2100.1I IT Security Policy.

7. Penalties.

Penalties for offenses not listed in the directive CPO 9751.1 Maintaining Discipline should be determined by reference to the penalties listed for offenses of a similar type or of comparable seriousness.

a. Types of delinquency or misconduct. Appendix 1 of CPO 9751.1 Maintaining Discipline is the Penalty Guide. Table 1, Paragraph 15 of that guide states, "Failure through willfulness or with reckless disregard for the regulations, to observe any security regulation or order prescribed by the competent authority. Investigations of security violations must be done initially by security managers in accordance with ADM P 1025.2C, ch-8." The Guide continues with the following penalty guidance:

(1) Where the violation involved information classified “below” Secret (such as Personally Identifiable Information) the recommendations are:

(a) The penalty for a first-time offense is reprimand to removal.

(b) The penalty for a second offense is suspension to removal.

(c) The penalty for a third offense is removal.

(2) Where the violation involved information classified Secret or “above” (assuming that this category encompasses a moderate or high-risk data breach) the recommendations are:

(a) The penalty for a first-time offense is reprimand to removal.

(b) The penalty for a second offense is removal.

8. Criminal penalties.

The Privacy Act of 1974, as amended, lists the following criminal penalties in sub-section (i).

a. Any officer or employee of an agency, who by virtue of his employment or official

position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by the Privacy Act or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

b. Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000.

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

9. References.

The following informational material is relevant to this topic.

a. Privacy Act of 1974 http://www.justice.gov/opcl/privacyact1974.htm

b. OMB Memo M-07-16 (May 22, 2007) Safeguarding Against and Responding to the Breach of Personally Identifiable Information http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

c. HCO 9297.2B GSA Information Breach Notification Policy (March 24, 2011) https://insite.gsa.gov/portal/content/520570

d. IT Security Procedural Guide: Handling IT Security Incidents CIO-IT Security-01-02 (April 22, 2008) http://insite.gsa.gov/graphics/staffoffices/incidentguide.doc

e. CIO 2100.1I GSA Information Technology (IT) Security Policy http://insite.gsa.gov/graphics/staffoffices/itsecuritypolicy1e.pdf)

f. 2104.1A GSA IT General Rules of Behavior http://www.gsa.gov/portal/directive/d0/content/533042

g. CPO 9751.1 Maintaining Discipline https://insite.gsa.gov/portal/content/523318

g. Federal Information Security Management Act (FISMA), http://csrc.nist.gov/groups/SMA/fisma/index.html

h. OMB Memorandum M-10-23 (Guidance for Agency Use of Third-Party Websites and Applications – June 25, 2010) http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

i. OMB Memorandum M-06-19 (July 12, 2006) Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-19.pdf