



## UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

### PERSONALLY IDENTIFIABLE DATA REMOVAL POLICY OCIO-6014-09

**Date of Issuance:** May 22, 2009  
**Effective Date:** May 22, 2009  
**Review Date:**

#### TABLE OF CONTENTS

#### Section

- I. PURPOSE
- II. AUTHORITY
- III. SCOPE
- IV. DEFINITIONS
- V. POLICY
- VI. RESPONSIBILITIES
- VII. EXCEPTIONS
- VIII. EFFECT ON OTHER POLICIES

#### **I. PURPOSE**

This document establishes policy within the United States Patent and Trademark Office (USPTO) for the removal of Personally Identifiable Information from USPTO premises.

#### **II. AUTHORITY**

- The protection of the USPTO systems and their data is required by Office of Management and Budget (OMB) Circular A-130; the Federal Information Security Management Act of 2002 (FISMA); and the Privacy Act of 1974.
- National Institute of Standards and Technology guides (800 Series) that provide the minimum security requirements for agency systems and major applications.
- OMB Memorandum M-06-16, which indicates that the extracts from databases which contain personally identifiable information (PII) may be in need of further protection if the extracts are removed from the USPTO premises.

#### **III. SCOPE**

The provisions of this policy apply to all USPTO employees and contractor employees using or operating USPTO computer systems and to contractor employees providing services to the USPTO who use USPTO Automated Information Systems (AISs) and networks. This policy applies to all USPTO AISs or resources, independent of size. For example, it applies to desktops, laptops, personal data assistants (PDAs), servers, and network devices to include firewalls, intrusion detection systems, intrusion

## PERSONALLY IDENTIFIABLE DATA REMOVAL POLICY

prevention systems, routers and switches. Additionally, this policy applies to all types of media used to record USPTO data which includes, but is not limited to: hard drives, CDs, DVDs, other magnetic media such as floppy disks, and solid-state media (flash memory, memory stick, USB flash drive, etc.).

This policy also applies to those AISs operated and used by contractor employees, guest researchers and collaborators to carry out the USPTO mission, whether or not they are owned, leased, or on Government property.

### **IV. DEFINITIONS**

For purposes of this policy, a data extract is defined as multiple records of information that are downloaded or copied from an USPTO database system (such as the PALM, Human Resources and the payroll system) and maintained in electronic format outside of the originating system. This policy is limited to data extracts that contain personally identifiable information (PII) that is considered to be protected (see USPTO Privacy Policy), such as Social Security Numbers, medical information, and certain information from charges, complaints, or cases that are not yet filed in court. This policy is additionally limited to data extracts that are physically removed from USPTO premises via electronic transmission, laptop, file, CD, diskette, memory key, or any other portable storage device. It additionally includes data extracts downloaded via USPTO's virtual private network (VPN) to any external device. Using the VPN to access files and data (without download to an external device) is NOT subject to this policy.

The risks from extracted personal data can be reduced in several ways:

- If the sensitive data is not needed in the extract, do not include it.
- Limit the number of records in the extract to the smallest number needed.
- Delete the extract as soon as it is no longer needed.

An example of what is NOT considered a data extract under this policy is the download of name and address information for correspondence purposes. In addition, accessing and working with files and information across PTONet or the VPN is NOT considered a data extract. However, if a user physically downloads (transfers) multiple records from an internal USPTO database system to a remote laptop or storage device through the VPN; this is considered a data extract.

Individual electronic documents that are not created through a database extract process (as defined above) are not considered a "data extract" for purposes of this policy and do not require the logging procedures outlined below in section III. This includes working files maintained on office workstations. However, if the individual files contain sensitive PII, the files should be protected prior to removal from an USPTO facility. Download and storage within the "My Documents" directory on a properly configured USPTO laptop or to an encrypted and password protected portable device, fulfills the security requirement for these files. Encrypting and password protecting the file(s), prior to download/removal, also fulfills the requirement. If there are any questions, on how to encrypt an individual file or group of files, please contact the USPTO Help Desk.

## PERSONALLY IDENTIFIABLE DATA REMOVAL POLICY

### **V. POLICY**

Procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

1. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
2. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.
3. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
4. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO VPN.
5. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.
6. Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external e-mail address via the Internet. The password key should be forwarded to the recipient in a separate e-mail from the attached file.

The automatic on-line remote back-up of network servers is excluded from the extract logging requirement.

### **VI. RESPONSIBILITIES**

All USPTO employees and contractor employees shall adhere to this policy and shall not engage in any activity that might circumvent its provisions. All USPTO employees or contractor employees responsible for the management, implementation, installation, configuration, operation, maintenance, or security of a USPTO AIS or network must implement the mandatory practices of this policy and must identify any proposed deviations from the mandatory practices of this policy and request a waiver in writing from the USPTO Policy, Privacy, and PKI Division (PPPD) in accordance with the waiver process as defined in the USPTO IT Security Handbook.

The IT Security Management Group (ITSMG) shall be responsible for monitoring user compliance with this policy as part of the periodic IT security self-assessment program or AIS evaluations and maintaining current, approved waivers as part of the documentation for appropriate system security plan(s). The PPPD is responsible for maintaining and updating this policy; reviewing, approving or denying waivers; and, monitoring compliance through bi-annual compliance reviews.

System owners shall implement the mandatory practices of this policy for each USPTO AIS for which they are responsible, unless a system is covered by a current, approved waiver. *USPTO's AAO 212-4*,

## PERSONALLY IDENTIFIABLE DATA REMOVAL POLICY

*Section III, IT Security Roles and Responsibilities*, identifies key USPTO roles that have both IT Security and C&A responsibilities.

Compliance with this policy shall be enforced through oversight, inspection, administrative, disciplinary, and corrective actions. As part of this policy, a USPTO Senior Privacy Official must be designated to oversee all issues specific to privacy information and compliance.

The USPTO Help Desk (HDS) shall create incident records upon being informed of a suspected loss or compromise of privacy information. The USPTO Help Desk shall inform the Office of Corporate Services upon notification of loss or theft of IT systems suspected of housing privacy information. The USPTO Help Desk shall also inform the USPTO Computer Incident Response Team (CIRT) upon notification of suspected compromise of privacy information.

The Administrative Management Group (AMG) shall be responsible for ensuring IT procurement contracts explicitly refer to this policy and that contractors are in compliance.

All incidents involving loss or compromise of PII shall be reported by the USPTO CIRT to the DOC IT CERT, who in turn informs the US-CERT within one hour of discovering the incident. Please refer to the *U.S. Department of Commerce, IT Security Program Policy and Minimum Implementation Standards* and the upcoming Breach Notification Policy for additional process guidance.

### **VII. EXCEPTIONS**

Additional exceptions to this policy shall be determined on a case-by-case basis using the waiver process as defined in the USPTO IT Security Handbook.

### **VIII. REFERENCES**

- *E-Government Act (Public Law 107-347), Title III - Federal Information Security Management Act (FISMA)*, December 2002.
- Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, February 2004.
- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, Revised November 2000.
- OMB M-03-22 *Guidance for implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 2006.
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 2006.

PERSONALLY IDENTIFIABLE DATA REMOVAL POLICY

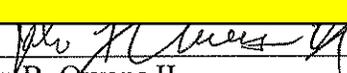
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007
- The Privacy Act of 1974, 5 U.S.C. §552a
- U.S. Department of Commerce, *IT Privacy Policy*.
- U.S. Department of Commerce, *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005.
- U.S. Patent and Trademark Office, *Agency Administrative Order 212-4, USPTO IT Security Handbook*.
- U.S. Patent and Trademark Office, *IT Privacy Policy*.
- U.S. Patent and Trademark Office, *Rules of the Road*.
- U.S. Patent and Trademark Office, *Comprehensive Records Schedule*.

**IX. EFFECT ON OTHER POLICIES**

This policy affects all new, revised, or retired policies issued in Fiscal Year 2009.

ISSUED BY:

ISSUED BY: John B. Owens II, CIO, USPTO  
(Signature)

  
\_\_\_\_\_  
John B. Owens II  
Chief Information Officer  
United States Patent and Trademark Office

OFFICE OF PRIMARY INTEREST: IT Security Management Group