



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

USPTO ENTERPRISE SHAREPOINT POLICY

OCIO-5003-09

Date of Issuance: April 27, 2009

Effective Date: April 27, 2009

Review Date:

TABLE OF CONTENTS

- I PURPOSE
- II SCOPE
- III DEFINITIONS
- IV POLICY
- V RESPONSIBILITIES
- VI EFFECT ON OTHER POLICIES
- VII ISSUED BY

I PURPOSE

This policy addresses the United States Patent and Trademark Office (USPTO) enterprise SharePoint environment. It provides a framework for the administration, maintenance, and support, establishes lines of ownership for both business and technical teams, and identifies the organizations that are responsible for various functions of the system. This policy also establishes rules for appropriate use of the enterprise SharePoint environment.

II SCOPE

This document establishes policies and responsibilities for the use and management of the USPTO enterprise SharePoint environment. These policies affect the Office of the Chief Information Officer (OCIO) and each agency business area that uses the enterprise SharePoint tools to support their mission.

ENTERPRISE SHAREPOINT POLICY

III DEFINITIONS

Personally Identifiable Information (PII)

PII is broadly defined as information that can be traced back to a specific individual. Employees must distinguish between Protected PII and Publicly Releasable PII. All information identifiable to a specific individual is protected PII unless listed as publicly releasable PII.

Examples of protected PII include but are not limited to the following:

- ◆ Home address, home phone number, personal e-mail address, place of birth, date of birth, Social Security number, maiden name, mother's maiden name, etc
- ◆ Human Resources information (including employment records, performance, criminal and medical information and history)
- ◆ Financial data (for individuals and businesses) such as: credit card/banking numbers, direct deposit information and associated data
- ◆ Biometric data
- ◆ Security clearance information

Examples of Publicly Releasable PII include the following:

- ◆ Non-financial information regarding business entities, such as: business names, business addresses, telephone numbers, web sites, e-mail, etc
- ◆ All information that has been publicly released, including information available on the USPTO public Web site (employee name, identification number, phone number, office, etc)
- ◆ Published patent applications,¹ which includes any data that may be included within the application
- ◆ Trademark applications

Records

Records include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them.

- ◆ Electronic recordkeeping system: An electronic system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

¹ While unpublished patent applications are not protectable as PII, this information is not public information, and is protected by 35 USC 122 (pre-publication protection) and 35 USC 181 (secrecy orders).

ENTERPRISE SHAREPOINT POLICY

- ◆ Recordkeeping system: A manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

IV POLICY

This section provides the USPTO policy on use of the agency's enterprise SharePoint environment. Policy guidance is broken into five components as follows.

General Policies

- ◆ USPTO will maintain a single, technical infrastructure to support the agency's aggregate requirements for SharePoint services while decentralizing the administration and management of individual SharePoint sites to agency business areas.
- ◆ SharePoint sites may be configured by business units using out of the box functionality. OCIO must approve the use of customized code that alters the underlying SharePoint code to prevent changes that will complicate normal patch and upgrade functions and potentially impact the security posture of the system.
- ◆ Access to SharePoint is limited to users on PTONet only. Access from outside of PTONet is not permitted.

Records Management

SharePoint is not authorized for electronic records management functions at USPTO. Information that is designated as official agency records must be maintained following approved records management and storage procedures.² Documents created in SharePoint that meet the definition of a record must be managed following the established procedures.

The USPTO has established enterprise system requirements for electronic record keeping systems. Electronic tools are available to assist in meeting business area needs for maintaining electronic records in their native format. Options also exist for compliance through paper-based storage methods. Employees are reminded to follow the *USPTO Rules of the Road*, Rule #2.

Controlled Unclassified Information

Controlled unclassified information shall not be posted to USPTO's SharePoint sites unless OCIO approved access and management controls are in place.

² Relevant Records Management Policies and Procedures: U.S. Patent and Trademark Office Comprehensive Records Schedule; Department of Commerce Records Management Policy, Department of Commerce Administrative Orders DAO 205-16, DAO 205-1; Federal Regulations, including 36 CFR §1234 Electronic Records Management, 36 CFR §1220.36 Maintenance and use of records; AAO-202-735 Limited Personal Use of Government Equipment.

ENTERPRISE SHAREPOINT POLICY

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) shall not be posted to USPTO's SharePoint sites unless OCIO approved access and management controls are in place.

Document Management and Workflow

SharePoint has many features for sharing information and facilitating collaboration across teams and organizations. These features include document posting, document check-out and check-in, automatic notification of changes to user groups, and online tracking of comments and approvals. In contrast, USPTO has invested in Documentum to provide enterprise document management, workflow, and records management services associated with agency business processes and automated information systems (AISs). There are distinct differences between the approved uses of these two products.

Agency wide use of the collaboration capabilities of SharePoint is encouraged as they enhance the organization's collaboration efficiency and effectiveness. However, SharePoint shall not be used to duplicate the document management, workflow, and records management functions of Documentum and shall not be integrated into agency AISs as a document management, workflow, or records management tool. Integration of SharePoint with Documentum to share documents or create electronic records is an approved practice.

Documents created and/or transmitted in SharePoint may be subject to discovery in Federal court litigation and to production pursuant to Freedom of Information Act requests. It is incumbent upon SharePoint users to effectively delete superfluous, non-relevant information and correspondence promptly to ensure that use of SharePoint results in enhanced efficiency and effectiveness and to prevent such information from resulting in duplicative or unnecessary sources of information.

Security Breach Notification: Incident Reporting and Handling

Incidents shall be reported and handled according to currently established USPTO policy. For full information please see the *Breach Notification Policy*.

Employees and/or contractors must notify their supervisor(s) or other appropriate supervisory channels when they become aware of security incidents,

Personally Identifiable Information (PII)

Effectively safeguarding and reporting breaches specific to Personally Identifiable Information (PII) is the responsibility of all USPTO employees and contractors. Established USPTO procedures shall be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises.

For additional information, including the removal of Personally Identifiable Information please see the *Personally Identifiable Data Removal Policy*.

ENTERPRISE SHAREPOINT POLICY

V RESPONSIBILITIES

OCIO Responsibilities

- ◆ Maintain agency technical procedures and security policies related to all SharePoint sites and appropriate access controls.
- ◆ Maintain a shared technical infrastructure to host agency SharePoint sites.
- ◆ Provide daily operations of the technical infrastructure (hardware, telecommunications, back up and recovery, Commercial off the Shelf (COTS) software and associated help desk functions).
- ◆ Install Operating Systems, COTS, SharePoint upgrades, and security patches.
- ◆ Plan and manage routine end-of-life replacement of hardware.
- ◆ Provide configuration management support for common services, including the monitoring and removal of unused sites and storage.
- ◆ Provide the following account administration services:
 - ◇ Create and manage data storage allocations for each business area.
 - ◇ Establish and maintain administrator privileges.
- ◆ Monitor system operation for integrity and availability.

Business Area Responsibilities

- ◆ Comply with all the policies in this document.

Note: Business areas may develop additional policies related to their individual implementations for further clarity, but in no case may the additional policy provide fewer restrictions than this main policy.
- ◆ Specify, establish and manage their internal SharePoint sites.
- ◆ Ensure that employees are adequately trained to assume administrator and related user roles.
- ◆ Request OCIO to establish business unit access and allocate space for the business area to create their own sites.
- ◆ Provide training regarding OCIO policy for SharePoint.

ENTERPRISE SHAREPOINT POLICY

VI EFFECT ON OTHER POLICIES

This policy has no direct impact on any other OCIO policies.

This policy is fully compliant with the following OCIO policies and laws including the following:

35 USC 122 (pre-publication protection)

35 USC 181 (secrecy orders)

AAO-202-735 Limited Personal Use of Government Equipment

Department of Commerce Records Management Policy

Department of Commerce Administrative Orders DAO 205-16, DAO 205-1

Federal Regulations including 36 CFR §1234 Electronic Records Management, and 36 CFR §1220.36 Maintenance and use of records

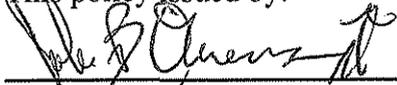
U.S. Patent and Trademark Office Comprehensive Records Schedule

USPTO Rules of the Road

USPTO Security Policies

VII ISSUED BY

This policy issued by:



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

OFFICE OF PRIMARY INTEREST: Program Management Group