



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

IT SECURITY EDUCATION AWARENESS TRAINING POLICY OCIO-6009-09

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. REFERENCES
- IX. EFFECT ON OTHER POLICIES

I. PURPOSE

This document establishes the uniform policy within the United States Patent and Trademark Office (USPTO) for Information Technology (IT) security training and awareness. This policy also establishes minimum standards for mandatory periodic training in IT security user awareness including accepted computer security practices of all users. The Department of Commerce has identified two requirements specific to Security Awareness and Training:

The USPTO shall develop, disseminate, and periodically review/update:

1. A formal documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. A formal, documented procedure to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

II. AUTHORITY

This policy is issued pursuant to:

- The Federal Information Management Security Act of 2002 (FISMA)

IT SECURITY EDUCATION AWARENESS TRAINING POLICY

- USPTO IT Security Policy Management Policy

III. SCOPE

The provisions of this policy apply to all USPTO employees and contractor employees using or operating USPTO computer systems, and to employees of contractor systems owned and operated on behalf of the USPTO. The scope of this policy is limited to security awareness and security training.

IV. DEFINITIONS

Awareness: Awareness is not training. Awareness focuses attention on security and is intended to allow individuals to recognize security concerns and respond accordingly. It is a state whereby a user is familiar with IT security, policies, practices, and procedures that are required of him/her to operate a workstation, server or other automated device in a secure environment.

Training: Training strives to produce relevant and needed security skills and competency in practitioners of functional specialties other than IT security (e.g., management, system design, acquisition, auditing). The content of training programs is designed to the requirements of specific target audiences. The goal of training is to build knowledge and skill to facilitate job performance.

Education: Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multi-disciplinary study of concepts, issues, and principles, and strives to produce IT security specialists and professionals capable of vision and pro-active response. Note: The definition of “education” is included in this document to differentiate it from “training” and to reinforce the intent and scope of this policy.

Sensitive Information: Any information, the loss, misuse, or unauthorized access to or modification of that could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

V. POLICY

A. General Policy

USPTO requires users to complete an IT security awareness course annually. The objective of this course is to raise USPTO’s employees’ and contractors’ IT security awareness. Completion of this course facilitates user recognition of, and response to, security concerns. Additionally, the course familiarizes employees and contractors with USPTO IT security policies and procedures.

Attendance of an IT security awareness presentation, provided as part of a new employees orientation, is a mandatory prerequisite to receiving logical access to USPTO systems.

New users shall complete a formal IT security awareness course, provided via the Commerce Learning System, within 30 days of receiving logical access to USPTO systems.

IT SECURITY EDUCATION AWARENESS TRAINING POLICY

Employees of contractors whose IT systems are owned and operated on behalf of the USPTO and process, store or forward USPTO information shall complete annual security awareness training. The scope of this requirement is tightly coupled to the requirement for those contractors that are required to have a Certification and Accreditation (C&A) performed on their system(s). Contractors that have certified and accredited (C&A) their system also have the requirement for individuals accessing those systems to have completed an approved security awareness training course. These individuals may never need (or have) direct access to PTOnet and associated systems, but the requirement for security awareness course completion exists by extension. Contractors can meet this requirement by generating their own course (consistent with FISMA and NIST guidance) and submit it to ITSMG for approval or a contractor may use the USPTO's approved course in electronic or paper format to certify to ITSMG that their employees have completed the course.

All users shall complete an annual refresher security awareness course by September 30th of each year.

Attendance at all applicable IT security awareness and training activities shall be documented for each user.

Due to the aggregate impact of IT security and awareness activities on the Business Units, particularly the Patent and Trademarks businesses, mandatory annual IT security awareness activities shall be coordinated with the Heads of the Business Areas, and accommodations will be made for users' busy schedules. In all cases, awareness and training beyond that which is mandatory will be approved by the user's supervisor.

Users shall be solicited for ideas on how to improve information security. NOTE: USPTO employees and contractor employees should be encouraged to view IT security as a positive procedural tool for ensuring the confidentiality, integrity, and availability of USPTO AIS.

B. Annual Awareness Requirements

Each user (USPTO employee, contractor employees, and all other individuals using AIS resources) shall understand the basic purpose of the USPTO Information Technology Security Program and its implementation. At a minimum, the annual security awareness course shall include the following IT security components:

1. USPTO IT Security Policies
2. Common System Threats, Vulnerabilities, and Risks
3. Confidentiality, Integrity, and Availability
4. Password Security; Logging Off; Multiple Sign-on's
5. Appropriate IT Security Rules of Behaviors
6. Peer-to-Peer Software Restrictions
7. Malicious Software
8. E-mail Hoaxes
9. Back-ups (where appropriate)

IT SECURITY EDUCATION AWARENESS TRAINING POLICY

10. Internet Use
11. Software Licensing
12. E-mail Manners
13. Expectations of Privacy
14. Incident Handling and Reporting
15. Personally Identifiable Information Definition and Protection
16. Telecommunication Security
17. Network Overview
18. Remote Sign-on
19. Physical and Environmental Security
20. Information Accessibility, Handling, Labeling, and Storage
21. Disposal of Sensitive Information
22. Repercussions of Misuse of AIS Resources or Failure to Follow IT Security Policy
23. Disaster Recovery and Contingency Planning
24. Configuration Management and Controls
25. Copyright Compliance
26. Social Engineering Threats
27. Anti-virus Software
28. Information and Data Sensitivity

C. IT Security Awareness Reinforcement Activities

As part of an effective IT security training program, IT security awareness reinforcement activities will also be provided for all users. IT security awareness reinforcement activities will include, but are not limited to:

1. Distribution of AIS security pamphlets and flyers
2. Viewing of AIS security videos
3. Dissemination of security posters throughout the facility
4. Security articles in the site's newsletters, daily bulletins, web pages, etc.

D. Role-based Training

Specialized, role-based training shall be provided on an annual basis to employees who have the following positions:

IT SECURITY EDUCATION AWARENESS TRAINING POLICY

1. Executive Management Authority (authorizing official or business area head);
2. Security Management (Information Technology Security Officer, System Owners, C&A Program Managers, Information System Security Officers);
3. IT Management Support (legal staff, public affairs, procurement staff and Contracting Officers' Technical Representatives);
4. IT Support Staff (system administrator, help desk personnel, network administrator,)
5. Operational Managers and System Users

Training course content shall be tailored to a user's role.

E. Training Methods

IT security training will be presented using multiple mediums in various settings including, but not limited to, interactive computer sessions in the USPTO E-Learning Center (computer-based training) or in-classroom instruction (instructor led training).

Training methods will be tailored to effectively provide what the user needs to know to perform his or her duties and reflect the business rules of the USPTO. Training methods for members of the public shall be constrained by controls that allow access to the training.

F. Education and Professional Certification

Specialized IT security positions based on the roles in section D of this policy do not require professional certification. Specialized IT security positions shall be reviewed to ensure minimum knowledge, skill, and ability levels are met.

G. Implementation

Specific implementation details for this policy, including a role-based training curriculum, will be provided in additional Information Technology Security Standards (ITSS), Program Plans, and/or Security Bulletins.

H. Compliance

This policy is pursuant to Section 3544 of the Federal Information Security Management Act (FISMA) of 2002 – 44 USC 3544 requirement for agencies to “develop and implement an agency-wide information security program” that includes periodic mandatory IT security user awareness and role-specific training; and the Office of Management and Budget (OMB) Circular A-130, Appendix III that requires mandatory security training prior to granting access to AIS.

Compliance with this policy shall be enforced through oversight, inspection, and administrative, disciplinary, and corrective actions.

IT security awareness and training for USPTO personnel shall be audited, tracked, and reported on a regular basis to ensure compliance with this policy. Annual testing of personnel shall be performed to evaluate effectiveness and compliance.

IT SECURITY EDUCATION AWARENESS TRAINING POLICY

Users who refuse to engage in, or cannot meet the IT security awareness and training requirement may have access to information and IT resources suspended or terminated. This may result in personnel action if access is required for fulfillment of position responsibilities.

VI. RESPONSIBILITIES

The Under Secretary and the Deputy Director provide the high-level direction for carrying out the IT security mission. They are responsible for the USPTO IT Security Program, including IT Security Training. The authority for carrying out the IT Security Program is delegated to other USPTO officials within the USPTO.

All users and managers shall be aware of and observe the USPTO policy regarding IT security training and awareness.

The IT Security Officer shall establish procedures for IT security awareness and training program for all USPTO personnel, including role-based training.

It is the responsibility of all USPTO employees and contractor employees to adhere to this policy and to refrain from any activity that might circumvent this policy. End users must read and understand all applicable training and awareness materials.

The CIO shall ensure that a USPTO IT Security Training and Awareness Program is established under the lead of the ITSMG.

The USPTO ITSMG shall:

- Work with the Office of Training and Office of Human Resources to ensure implementation of the overall IT Security Training and Awareness Program
- Oversee the implementation of an IT Security Training and Awareness Program
- Determine the IT security training and awareness goals
- Ensure management support and appropriate funding
- Determine the content of the IT security training and awareness materials
- Ensure that all training materials are reviewed by the Business Units for compliance with the patent and trademark laws, policies and business rules
- Coordinate IT security training and awareness planning activities
- Conduct periodic reviews of compliance with USPTO IT security training and awareness policies
- Maintain and update the policy, review and approve or deny waivers, and monitor compliance through the conduct of annual compliance reviews
- Be responsible for monitoring system user compliance with this policy as part of the periodic IT security self-assessment program or automated system evaluations
- Maintain approved waivers as part of the documentation for appropriate system security plan(s)

IT SECURITY EDUCATION AWARENESS TRAINING POLICY

- Ensure that the IT Security Awareness and Training Programs are communicated to all USPTO users and contractor employees

The Office of Human Resources shall:

- Provide new USPTO users IT Security User Awareness material for their review
- Initiate courtesy union notifications for required training
- Facilitate disciplinary actions for violations of policy

Contracting Officers' Technical Representatives (COTRs) shall:

- Have contract oversight security responsibilities and ensure that contractor-related security requirements are followed throughout the contract life-cycle
- Ensure that contractor employees working for the USPTO receive annual User Awareness courses
- Ensure that technical personnel meet USPTO requirements for IT Security training and expertise before they start work

Violations of this policy are to be reported to the USPTO Helpdesk by calling 571-272-9000 or by email using the "Helpdesk 9000" email address in the Microsoft Outlook Global Address or helpdesk@uspto.gov. Incidents may be also forwarded to CIRT@USPTO.GOV.

VII. EXCEPTIONS

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.
- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- Federal Information Processing Standard (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.

IT SECURITY EDUCATION AWARENESS TRAINING POLICY

- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 2006.
- 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*.
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*.
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*.

IX. EFFECT ON OTHER POLICIES

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

ISSUED BY:



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

OFFICE OF PRIMARY INTEREST: IT Security Management Group