



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

PASSWORD PROTECTED SCREEN SAVER POLICY OCIO-6002-09

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 policy establishes a uniform practice within the United States Patent and Trademark Office (USPTO) for the protection of sensitive information and the prevention of intrusion and illicit use of any user's workstation or server through the use of password-protected workstation screen savers.

The use of password-protected screen savers is essential to ensure confidentiality of sensitive data that resides on workstations and/or servers. They reduce the possibility of unauthorized users gaining access to sensitive data through the automated information system (AIS) access provided by physical access to and use of the unattended unit. An unauthorized user or "hacker" having gained physical access to a logged-in workstation can quickly implement unauthorized remote access by installing a "back door" while the unit is unattended. They can later remotely access the unit, thereby giving them access to all USPTO automated information systems (AIS) and information that the user has access to, or at the very least copy sensitive and/or personal information from the compromised unit itself.

II. AUTHORITY

This policy is issued pursuant to:

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

PASSWORD PROTECTED SCREEN SAVER POLICY

III. SCOPE

The provisions of this policy apply to all USPTO employees and contractor employees using or operating USPTO AIS. This policy also applies to contractor employees providing telecommunications and AIS services to the USPTO.

IV. DEFINITIONS

Screen saver: A background application that displays an image (animated to prevent screen burn-in) that is activated on a workstation or server display when no user activity has been sensed for a pre-determined amount of time.

Personal or customized screen savers: A personal or customized screen saver is any screen saver that is not included with the manufacturer's operating system default installation.

Inactivity: Inactivity is that period of time for which there has been no interaction by the user with the computer using any input device (e.g., keyboard or mouse). Inactivity is not a measure of active applications or processes.

Locked workstation or server: A locked workstation or server is a computer that has activated the security mechanism to require the user to re-enter their user name and password to regain access to their computer. Locking the workstation does not prevent active applications or processes from completing their work. Applications and processes continue to work in the background unaffected by the operation of the screen saver or locked state of the computer. The use of the term 'workstation' is meant to include laptop systems regardless of the physical location of the laptop.

V. POLICY

When leaving their work area, even for a brief period of time, users should secure their workstation or system by simultaneously pressing the CTRL+ALT+DEL keys and then selecting the "Lock Computer" button. Timeout activated password-protected screen savers lock the computer after a set period of inactivity but are a failsafe in case the user forgets to manually lock the unit when leaving the work area. The user unlocks the system by simultaneously pressing the CTRL+ALT+DEL keys, then entering his/her PTOnet User Name and password.

When locked, the workstation can be unlocked only by the user or an authorized system administrator using their user ID and Password. Active applications, or processes and open files, are not affected during activation of the password-protected screen saver or when the unit is manually locked. Applications or processes continue to function and will continue to perform all tasks, including printing, while the screen saver is active or the workstation is locked. Recent work should be saved before locking via screen saver in case of a power failure, disk malfunction or other event that could cause loss of unsaved work. The approved workstation screen saver provided by the USPTO has no history of causing any loss of work.

Password-protected screen savers shall be implemented on all workstations and servers to ensure confidentiality of sensitive data that might reside on workstations and/or servers and to reduce the possibility of unauthorized users gaining access to sensitive data or resources through the use of an

PASSWORD PROTECTED SCREEN SAVER POLICY

unattended workstation or server. Enforceable technical controls shall be implemented effective days (30) business days following the issuance of this policy as follows:

- Technical controls shall be implemented to ensure password-protected screen savers are configured and enabled on all servers and workstations.
- Screen savers shall be automatically activated on all workstations after sixty (60) minutes of inactivity. Screen savers shall be activated on all servers after sixty (60) minutes of inactivity.
- The logon banner shall be displayed upon initial logon and before anyone attempts to unlock the computer after activation of the password-protected screen saver.
- The screen saver chosen must ensure the least impact to computing resources (e.g., memory and CPU utilization) to ensure active processes are not adversely impacted. This screen saver is part of the baseline install for USPTO workstations running Microsoft OS. If the screen saver is not active on your workstation, please contact the Help Desk.
- Downloaded screensaver software is prohibited from use, as this software may maintain malicious code or offensive images.
- Although much of this policy describes functionality commonly found in the Microsoft Windows family of operating systems, Unix and other AIS shall select an equivalent low-resource utilization screen saver for implementation on those AIS and be configured in a similar manner consistent with this policy.
- Screen saver configuration tabs should be disabled and hidden on workstations and servers using technical controls to prevent alteration to the configurations as specified in this policy.

Screen savers shall not terminate active user network sessions so as not to interfere with server-based, active unattended applications and/or processes.

VI. RESPONSIBILITIES

It is the responsibility of all employees and contractor employees to adhere to this policy by not altering the configuration of the password-protected screen saver to circumvent its protection of the workstations and servers.

It is the responsibility of system administrators to ensure technical controls are in place to enforce the configurations as specified in this policy.

Violations of this policy shall be reported via e-mail to the HELPDESK 9000 e-mail address.

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.

PASSWORD PROTECTED SCREEN SAVER POLICY

VIII. REFERENCES

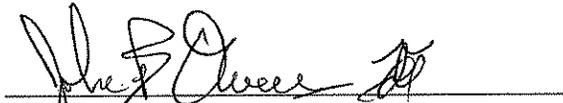
- *E-Government Act (Public Law 107-347), Title III - Federal Information Security Management Act (FISMA)*, December 2002.
- Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, February 2004.
- Federal Information Processing Standards (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.
- 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*.

IX. EFFECT ON OTHER POLICIES

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

PASSWORD PROTECTED SCREEN SAVER POLICY

ISSUED BY:

A handwritten signature in black ink, appearing to read "John B. Owens II", is written over a horizontal line.

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

OFFICE OF PRIMARY INTEREST: IT Security Management Group