



## UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

### PASSWORD MANAGEMENT POLICY OCIO-6012-09

**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**

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. Proper password management is required to ensure that only authorized users have access to a USPTO AIS (Automated Information Systems) and to prevent access by unauthorized persons.

Passwords are vital to computer security - they are the front line of protection for user accounts. A poorly chosen password may result in the compromise of USPTO's entire corporate network. As such, all USPTO employees (including contractors and vendors) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

#### **II. AUTHORITY**

This policy is issued pursuant to:

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

## PASSWORD MANAGEMENT POLICY

### III. SCOPE

Each USPTO AIS shall use passwords as a means for user authentication unless alternate access controls of equal or greater strength are implemented. AIS may also use biometrics or digital certificates to control access. The access controls implemented should provide security commensurate with the level of sensitivity of the AIS or of specific resources being accessed (i.e., information or special devices). All USPTO AIS and associated equipment that rely on passwords as the means to authenticate users shall implement effective password management in accordance with this policy.

The provisions of this policy apply to all USPTO employees and contractors accessing, using or operating USPTO workstations, servers or information systems and to contractors providing telecommunications and AIS services to the USPTO.

This policy also applies to those AIS owned and operated by contractors, its employees, USPTO guest researchers, collaborators, and other Federal agencies that carry out the USPTO mission, whether or not they are owned, leased, or on Government property. This policy must be explicitly addressed in all IT procurement activities. Those AIS intended to provide unrestricted access are excluded (e.g., public USPTO Web pages and kiosks).

### IV. DEFINITIONS

**Authentication:** The authentication mechanism provides assurance that the user really is who he/she says he/she is. Authentication consists of something a user knows (such as a password), something the user has (such as a token or smart card), or something the user is (such as a fingerprint). Strong authentication will use a combination of authentication factors (such as a SecureID number and a password).

**Encryption or Encrypted:** The process of transforming data (plaintext) to an unintelligible form (cyphertext) in such a way that the original data either cannot be obtained (one way hashing) or cannot be obtained without using the inverse decryption process (encryption).

**Management Controls:** Controls that address management of the security aspects of the AIS and the management of risk for the AIS. Management controls include risk management, review of security controls, AIS life cycle controls, processing authorization controls, and system security plan controls.

**Operational Controls:** Controls that address security mechanisms primarily implemented and executed by people (as opposed to AIS) acting in compliance with policy.

**Technical Controls:** Technical Controls consist of hardware and software controls used to provide automated protection to the AIS or applications. Technical Controls operate within the AIS.

**System Accounts:** Accounts which are used to run services on an operating system. They are not normally used by an individual to log on to a system.

### V. POLICY

#### Password Issuance

Initial passwords shall only be issued in person or by use of a callback procedure, or the equivalent, to a listed office work telephone number for the user requesting their password. When the initial password is

## PASSWORD MANAGEMENT POLICY

given over the telephone, user verification shall be made using the individuals' shared secret derived from approved user forms on file with the Help Desk. It is each user's responsibility to immediately log onto the AIS for which the password has been issued to take ownership of the account by changing the password.

An initial password is a password created and given to a user to enable initial access. Ownership of an account requires that personal passwords used to authenticate identity be known only to the individual who created the password.

Therefore, USPTO AIS shall force a new user to change their initial password supplied by a System Administrator upon initial access to an AIS and this requirement shall be enforced through management, operational and technical controls.

*Note: Passwords must NOT be left on a user's voicemail or provided to anyone else other than the account owner. Passwords must not be distributed through non-encrypted electronic mail, voice-mail, or left on answering machines.*

### **Password Protection and Storage**

Passwords must be protected to prevent unauthorized use. Specifically:

- Don't reveal a password to ANYONE
- Don't ever discuss passwords over the phone (initial password issuance is the one exception)
- Don't reveal a password in an email message
- Don't reveal a password to your supervisor, administrative assistant or clerical support person.
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or refer the issue to the USPTO Help Desk as a possible social engineering attempt . Do not use the "Remember Password" feature of applications (e.g., Outlook, Explorer).

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including PDAs or Blackberries).

### **AIS and Applications Requirements**

1. AIS and workstations must not display or print passwords as they are entered.

## PASSWORD MANAGEMENT POLICY

2. User applications must not be enabled to retain passwords for subsequent re-use, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for re-use. This does not include the USPTO enterprise single sign-on.
3. Store passwords, algorithms, keys, key generation material, certificates, codes, or other schemes that are used, maintained, or managed by the AIS for authentication purposes in encrypted form that prevents unauthorized individuals from gaining access to them.
4. Prevent the capture and viewing of passwords through operating system or software application features that may allow an individual access to a clear text password or a password in any form that can be captured and replayed.
5. Any operating system or software application “feature” that would allow a System Administrator to view personal passwords must be disabled.
6. Passwords, other than single-use (one-time) passwords, must be encrypted when transmitted across a wide area network or the Internet.
7. Passwords for access to individual workstations (PCs) (such as passwords for screen savers) shall be encrypted when stored electronically.
8. AIS shall be designed so that temporary User IDs, passwords, and parameters associated with other means of authentication shall be designed to automatically expire after a specific date or passage of a specific time period. If this is not technically possible the USPTO Waiver Policy should be followed.
9. Access scripts, macros, database connectors or other similar software or utility shall not contain passwords embedded in them unless they are compliant with NIST FIPS Publication 140-2, Security requirements for Cryptographic Modules, encryption standards for storing and transmitting the passwords.
10. Access to password files or password databases must be restricted to individuals authorized to manage the AIS.
11. Passwords for servers, mainframes, telecommunications devices (such as routers and switches), and devices used for IT security functions (such as firewalls, intrusion detection, and audit logging) must be encrypted when stored electronically.

In rare cases, minimum standards may not be attainable due to technical limitations with some operating systems and/or applications. In such cases, those features, which most closely attain adherence to the minimum standards articulated in this policy, shall be implemented in accordance with USPTO waiver process. The details of this process may be found in the USPTO IT Security Handbook.

### **Default Accounts and Passwords**

Operating systems, firewalls, databases, network devices and applications that have their own security subsystems are often configured with default administrative or other accounts. These accounts have well known documented default passwords associated with them that are readily available on the Internet or in system documentation.

## PASSWORD MANAGEMENT POLICY

Likewise, some COTS AIS have default passwords (such as vendor supplied passwords for training, field service or maintenance accounts). These will be changed immediately after installation and before an AIS becomes operational.

All unnecessary default accounts shall be disabled, when determined they are not necessary for operation of the AIS.

All default accounts shall be renamed and passwords shall be implemented for any null or carriage return character password accounts.

The default username(s) should also be renamed, if possible. In some situations, this is not possible due to specific AIS requirements.

### **Password Expiration, Aging, and Changes**

All passwords shall have a maximum life of 90 days.

AIS shall implement technical controls to have an automated mechanism to ensure that users are forced to change their passwords at an interval not greater than 90 days.

Technical controls shall be implemented to automatically remind users that the password expiration date is approaching. This reminder shall occur within a reasonable period before the 90-day period is over to provide the user an opportunity to change their passwords. Users must change their password sometime during this notification period. If users have not changed their password by that time the users access shall be temporarily suspended and shall be required to contact the Help Desk to assist them to reestablish access.

Service or system accounts, on which vital system processes are dependent for successful operation, are exempt from the above technical control requirement regarding automated mechanisms to change passwords. However, they are still required to be changed every 90 days.

- Passwords shall be changed immediately on direction from management.
- Anytime a password is suspected of being compromised or actually has been compromised (lost, forgotten, stolen), it shall be changed immediately or disabled until the password can be changed.

### **Reuse of Passwords and Password Uniqueness**

Passwords shall not be reused by repeating any of the last 8 passwords that have been used, nor shall the same password be reused within a 2-year period.

Although a password history is maintained by the AIS and the AIS may attempt to prevent the reuse of passwords, it is each user's responsibility to ensure that they do not make minor changes to their password to circumvent the intent of this policy. It is each user's responsibility to formulate unique passwords when prompted to do so.

Passwords used for general access shall be different than passwords used to access specific applications or other privileged access (e.g., System Administrators shall use designated administrative accounts for system administration tasks and a regular non-privileged account for general user access such as accessing e-mail, etc.).

## PASSWORD MANAGEMENT POLICY

Passwords used to access Internet or remote AIS shall be different from passwords used to access internal AIS and applications.

### **Technical Controls**

Technical controls shall be implemented to automatically maintain a history of the previously used 8 passwords to prevent the reuse of those passwords and to enforce the selection of policy compliant passwords to the extent possible.

AIS shall be designed so that temporary User IDs, passwords, and parameters associated with other means of authentication shall be designed to automatically expire after a specific period of time.

### **Password Composition**

The minimum length for passwords is eight (8) non-blank characters, and the maximum length is fourteen (14).

Privileged user or service accounts that have any administrative or elevated privileges on an AIS (e.g., enables them to control, configure the AIS, network infrastructure etc.) such as System Administrators, Network Administrators, Database Administrators and application developers are required to use passwords with a minimum length of fourteen (14) non-blank characters.

All PTOnet users shall be responsible for creating passwords comprised of a combination of letters and numbers, and may include special keyboard characters (i.e., asterisk, pound sign, exclamation point) as described below.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "USPTO", "patent", "trademark" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

The same character may not be used more than three times in the password (e.g., 'AAAAAAA1' is not acceptable, but 'A%rmp2g3' and 'A%ArmA2g3' are acceptable).

A good method for password selection is to pick a known phrase that can be remembered, then choose the first or last letter of the first eight words to be the password. For example, "In Xanadu did Kubla Kahn a

## PASSWORD MANAGEMENT POLICY

stately pleasure dome decree" becomes "IXdKKaspdd!." Titles and selected lines in a familiar song may be used in a similar manner.

All passwords must contain characters from at least 3 of the following 4 categories:

- English upper case letters: A, B, C.....Z
- English lower case letters: a, b, c.....z
- Westernized Arabic numerals: 0, 1, 2.....9
- Non-alphanumeric special characters (e.g., punctuation symbols such as ` ~ ! @ # \$ % ^ & \* ( ) \_ + - = { } | [ ] \ : " ; ' < > ? , . /)

DO NOT construct simple passwords as shown in the following examples, they are provided for *illustrative purposes only*.

Example of how to change your password in the future: (In the following example we will use October 2nd as your initial password change. Of course, this is only an example; you can change your password any way you like as long as you follow the strong password guidelines.)

- Pass-word1 (user changes password to this on October 2nd)
- Pass-w0rd2 (user changes password to this on January 2, 2001 - 90 days later)
- P@ss-w0rd3 (user changes password to this on April 2, 2001 - 90 days later)

Examples of adequate passwords:

- dygGine1 (8 characters using uppercase, lowercase, and numeric)
- K\*ceBoite (9 characters using uppercase, lowercase, and special character)
- wazii02Ofer (10 characters using uppercase, lowercase, and numeric)

Examples of inadequate passwords that will cause an error message:

- WindowsLinux (must also have either a number or a special character)
- AaaB53 (must have at least 8 characters and no more than 14)
- dgrtlo0n (must have at least one uppercase letter)

### **Technical and Other Controls**

AIS shall implement technical controls to enforce this Password Management Policy.

All PTONet users shall be responsible for creating passwords comprised of a combination of letters and numbers, or include special keyboard characters (i.e., asterisk, pound sign, exclamation point) as described above. Where technical controls are unable to enforce any requirement of this policy (e.g., the same character may not be used more than three times in the password), it is the responsibility of the user to ensure compliance with this policy.

## PASSWORD MANAGEMENT POLICY

### **Account Lockout**

Five (5) failed attempts to provide a legitimate password for access to an AIS should result in the user being disconnected from the service, and access to be suspended for at least three (3) minutes.

### **Temporary Accounts**

Management, Operational and Technical controls shall be implemented to disable accounts issued on a temporary basis. Procedures shall be used to identify expected account use duration upon requesting such accounts and the technical controls shall enforce account expiration by disabling the account automatically on a specified date. It is the responsibility of the user to which the account was assigned to request any extensions of temporary accounts expirations prior to the account expiring if one is necessary.

### **Group Passwords**

Group passwords are permitted for information systems placed within the production data center for local, console access only. Group passwords for remote connections, whether from public origins or from within the USPTO local area network, are prohibited unless a waiver is granted according the waiver process outlined in the USPTO IT Security Handbook.

## **VI. RESPONSIBILITIES**

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.

It is the responsibility of System Administrators to ensure technical controls and/or operational procedures are in place to identify, prevent, correct, and report violations of this policy.

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

ITSMG maintains and updates this policy annually, reviews and approves or denies waivers, and monitors compliance through the conduct of annual compliance reviews.

Each AIS Information System Security Officer (ISSO) shall implement the mandatory practices of this policy for all USPTO AIS they are responsible for that are not covered by an approved waiver.

Any USPTO employee or contractor employee responsible for the management, implementation, installation, configuration, operation, maintenance or security of a USPTO AIS shall 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 ITSMG.

The ITSMG shall ensure communication of the policy to all USPTO employee and contractor employee AIS users and shall ensure that IT security awareness and training programs address password management.

System Owners shall be responsible for the monitoring of AIS user compliance with this policy as part of the periodic IT security self-assessment program or automated AIS evaluations, and maintain approved waivers as part of the documentation for appropriate system security plan(s).

## PASSWORD MANAGEMENT POLICY

### **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.
- 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 Memorandum M-03-22 *Guidance for implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB M-06-15, *Safeguarding Personally Identifiable Information*, May 2006.
- OMB M-06-16, *Protection of Sensitive Agency Information*, June 2006.
- OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.
- OMB 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*.

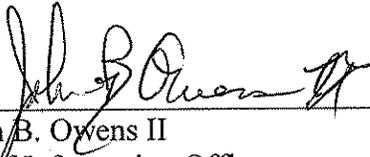
PASSWORD MANAGEMENT POLICY

- 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:



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

OFFICE OF PRIMARY INTEREST: IT Security Management Group