



S T A T E O F M A R Y L A N D  
DEPARTMENT OF INFORMATION TECHNOLOGY

## **Password Policy & Guidance**

### **1.0 Overview**

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of an agency's entire network. As such, all DoIT employees (including contractors and vendors with access to DOIT systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

### **2.0 Purpose**

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

### **3.0 Scope**

This guidance applies to all DoIT employees, staff subordinate to DoIT contracts, as well as any individual using DoIT resources. This guidance applies to all network and computer systems (desktops, workstations, laptops, servers, firewalls, hubs, switches, and remote access devices) in the Local Area Network and stand-alone computers.

### **4.0 Policy**

The following is general password policy applicable for most systems:

- Passwords and user logon IDs will be unique to each authorized user;
- The minimum length for passwords varies for each application. For some applications it will consist of a minimum of 6 alphanumeric characters (no common names or phrases). Others will be a minimum of 8 alphanumeric case-sensitive characters. Under no circumstance is any password to be shared with anyone else;
- The root or administrator user has a minimum password length of 8 characters and must be changed at least annually by the system administrator;
- System passwords will be changed immediately upon termination/resignation of any employee with administrative access;
- Regular users, Root and Administrators must have at least one non-letter character in their password;
- Passwords shall not be shared or coded into programs;
- User Passwords will be changed at least annually. Most systems can enforce password change with an automatic expiration and prevent repeated or reused passwords. If the system does not, the responsibility falls upon the user to change after 365 days;

- Password history should not allow users to reuse any password for one (1) year;
- Users are not allowed to use common words and are never based on personal information, (i.e. username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.);
- User accounts will be disabled after 3 failed login attempts;
- Sessions will be suspended after 15 minutes (or other specified period) of inactivity and require the password to be reentered;
- Logon IDs and passwords should be suspended after a specified period of non-use;
- Users should be removed or disabled in a timely fashion upon termination of employment;
- Logon-ids and passwords are to be used only by the person to whom they were issued; and
- Personal passwords shall be distributed from the password source in a way that only the intended recipient can view it

## **5.0 Guidance Statement**

User accounts are provided for the purpose of conducting the business of this Agency and supporting the mission of each department. Computers and networks provide access to local and remote resources, as well as the ability to communicate with other users worldwide. Such open access is a privilege requiring individuals to act responsibly. Users must respect the rights of other users, the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

## **5.1 General Password Construction Guidelines**

Strong passwords have the following characteristics:

- Contain both upper and lower case characters;
- Have digits and punctuation characters as well as letters e.g.,  
0-9,!@#\$\$%^&\*()\_+|~=-\`{ }[]:"';<>?,./) ;
- Are at least eight alphanumeric characters in length;
- Are not a word in any language, slang, dialect, jargon, etc.;
- Are not based on personal information, names of family, etc.;
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

## **5.2 Password Protection Standards**

Do not use the same password for agency accounts as for other non-agency access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various agency access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential agency information.

Do not:

- reveal a password to the boss
- talk about a password in front of others
- hint at the format of a password (e.g., "my family name")
- reveal a password on questionnaires or security forms
- share a password with family members
- reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Internet Explorer, Outlook, etc...).

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to OIT and change all passwords.

#### **Application Development Standards**

Application developers must ensure their programs contain the following security precautions.

Applications should:

- support authentication of individual users, not groups;
- not store passwords in clear text or in any easily reversible form;
- provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password;
- support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

#### **Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.