

<b>NORTH CAROLINA DEPARTMENT OF COMMERCE</b>	<b>Policy # MIS-4</b>
<b>TITLE: Password Requirements Policy</b>	
<b>Effective Date: July 1, 2005</b>	<b>Administering Authority:</b>
<b>Revisions:</b>	<b>Management Information Systems</b>
<b>Statutory Authority: N/A</b>	

### **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 the NC Department of Commerce's entire network. As such, all NC Department of Commerce employees (including contractors and vendors with access to NC Department of Commerce 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 creation of strong passwords, the protection of those passwords, and the frequency of change.

### **3.0 Scope**

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any NC Department of Commerce facility, has access to the NC Department of Commerce network, or stores any NC Department of Commerce information.

### **4.0 Policy**

#### **4.1 General**

- All production system-level passwords must be part of the NC Department of Commerce MIS administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every forty two (42) days. You will be prompted by the system when 42 days have passed without a change to your password. Failure to change your password when you receive this prompt will result in suspension of your account. You must contact NC Department of Commerce's MIS helpdesk to have your account re-activated when this occurs.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

#### **4.2 Guidelines**

##### **A. General Password Construction Guidelines**

Passwords are used for various purposes. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local equipment logins.

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.
  - 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)

#### **COMMERCE SYSTEM PASSWORDS MUST BE COMPOSED AS FOLLOWS:**

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#%&^\*()\_+|~- =\`{}[]:~<>?,./)
- Are at least eight alphanumeric characters long.
- 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.

NOTE: Do not use either of these examples as passwords!

#### **B. Password Protection Standards**

Do not use the same password for NC Department of Commerce accounts as for other non- NC Department of Commerce system access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various NC Department of Commerce access needs. For example, select one password for the accounting system and a separate password for your network logon.

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

Here is a list of "dont's":

- Don't reveal a password to ANYONE
- Don't reveal a password in an e-mail message
- 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 reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them contact NC Department of Commerce's MIS helpdesk for assistance.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

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 NC Department of Commerce's MIS Security officer and change all passwords immediately.

Password cracking or guessing may be performed on a periodic or random basis by NC Department of Commerce MIS staff. If a password is guessed or cracked during one of these scans, the user will be required to change it.

### **C. Application Development Standards**

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

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should 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.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

### **5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action consistent with Office of State Personnel and NC Department of Commerce policy, up to and including termination of employment.

### **6.0 Definitions**

#### **Terms**

#### **Definitions**

Application Administration Account Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

### **7.0 Revision History**