



Office of the Governor
State Chief Information Officer

Security Standard

Title: User ID and Password Protection Standard

Scope: The standard applies to all state agencies, departments, institutions, commissions, committees, boards, divisions, bureaus, offices, officers, and officials of the State. The standard does not apply to the General Assembly, the Judicial Department, or The University of North Carolina and its constituent institutions, unless they elect to participate in the information technology programs, services, or contracts offered by the Office of Information Technology Services (ITS).

1.0 Rationale

To reduce unauthorized access to information technology systems.

2.0 Enterprise Wide Standard

The use of passwords in conjunction with unique user IDs is required to control authorized access as well as to reduce unauthorized access to the state's information technology systems and applications. With the exception of password composition, the enterprise standard rules apply to all user ID and password construction and management. Password composition rules vary based upon the associated levels of risk.

Password composition and management are governed by the standards set forth below.

2.1 Enterprise Standard Rules - User ID Composition

1. Each user shall be uniquely identified to a system or an application with an ID that is associated only with that user. This does not apply to system administration accounts which may operate under different rules.
2. User IDs for internal state systems, to the extent possible, shall be different from user IDs for external, non-state resources.

2.2 Enterprise Standard Rules - User ID Management

1. User IDs shall be disabled promptly upon a user's termination from work for the State or upon the cessation of a user's need to access a system or application.
2. Where possible, unsuccessful logon attempts shall be limited to three before the user logon process is disabled.
3. User IDs that are inactive for 45 days must be disabled, except as specifically exempted by the security administrator. User IDs that are inactive for 18 months must be completely removed from the system, except as specifically exempted by the security administrator.

4. Only authorized system or security administrators and help desk staff shall be allowed to enable or re-enable a user ID, except in situations where a user can do so automatically through challenge/response questions.
5. Agencies must identify a backup system administrator to assist with user ID management when the primary system administrator is unavailable.

2.3 Enterprise Standard Rules – Password Composition

1. For secured access to systems and applications, such as electronic mail and LAN access, passwords shall have at least six characters of any sort.
2. For access to all systems and applications that require a high level of security, such as electronic fund transfers, taxes, and credit card transactions, passwords shall be at least 8 characters.
3. To the extent possible passwords shall be composed of a variety of letters, numbers and symbols¹ with no spaces in between.
4. To the extent possible, passwords shall be random characters from the required categories of letters, numbers and symbols.
5. Passwords shall not contain dictionary words or abbreviations.
6. Passwords shall not contain number or character substitutes to create dictionary words (e.g., d33psl33p for deep sleep²).
7. Passwords for internal state resources shall be different from passwords for external, non-state resources.
8. Password generators that create random passwords are allowed.
9. Password management application features that allow users to maintain password lists and/or automate password inputs are prohibited, except for simplified/single sign-on systems approved by the State Chief Information Officer (State CIO).

2.4 Enterprise Standard Rules - Password Management –

1. Except as specifically allowed by the security administrator, passwords shall not be revealed to anyone, including a supervisor, family members or co-workers. In special cases where a user must divulge a password, such as for system support, the user shall immediately change the password after the purpose for revealing the password has been achieved.
2. Users shall enter passwords manually, except for simplified/single sign-on systems that have been approved by the State CIO.
3. No automated password input is allowed, except for simplified/single sign-on systems that have been approved by the State CIO.

¹ Valid symbols are @, \$, +, -, #, ?, ., !, %, and _ . In RACF, the first character of a password must be a letter.

² Other number/symbol for letter examples are 0 for o, \$ or 5 for \$, 1 for i, and 1 for l, as in capta1n k1rk or mr5pock.

4. Passwords shall not be stored in clear text on hard drives, diskettes, or other electronic media. Passwords can be stored in encrypted format.
5. Individual user passwords (e.g., e-mail, web, and calendar) used to access systems and applications shall be changed at least every 90 days. Passwords cannot be re-used until six additional passwords have been created.
6. Passwords shall not be inserted into e-mail messages or other forms of electronic communication without proper encryption. Conveying a password in a telephone call is allowed when a positive identification has been established.
7. Where possible and practicable, access to password protected systems shall be timed out after an inactivity period of 30 minutes or less or as required by law, if the inactivity period is shorter than 30 minutes.
8. Passwords shall not be displayed in clear text during the log on or other processes. Where possible, applications that require clear text authentication shall be converted to equivalents that can use encryption.³

3.5 Enterprise Standard Rules - Password Management - System Administrators

1. All passwords (e.g., Unix, NT, and RACF) shall be changed at least every 90 days. Administrative user accounts and accounts with special privileges shall be changed at least every 30 days.
2. A user account that has system-level privileges or programs such as root access shall have a unique password from all other accounts held by that user.
3. Password files shall be retrievable only to the security administrator or a designated backup security administrator.

Vendor supplied default and/or blank passwords shall be immediately identified and reset as soon as an information system is installed.

³ Encryption is defined in the Security Architecture Chapter, Standard 3 "Use Cryptography based on Open Standards."