



State of North Carolina  
Department of Public Safety  
POLICIES & PROCEDURES

## INFORMATION TECHNOLOGY

*Division:* ADMINISTRATION  
*Chapter:* INFORMATION  
TECHNOLOGY  
*Policy:* NETWORK USE  
*Issue Date:* OCTOBER 2, 2012  
*Revised:*

### I. PURPOSE

Access to the Department of Public Safety's (DPS) systems requires that specific user responsibilities be enforced to ensure adequate network security. This policy informs the user of his or her responsibilities when using the Department's network.

### II. SCOPE

This policy applies to all employees, including permanent, contractual, and consultant employees who work for the Department of Public Safety and use the Department of Public Safety computing and networking resources. All users are expected to become familiar and comply with the guidance provided herein. Questions regarding this policy should be directed to the Department of Public Safety's Information Security Office (Statutory and/or Regulatory Authority: Statewide Information Security Manual; § 147-33.110).

### III. POLICY

1. Passwords. The following guidelines regarding password security shall be followed at all times:
  - a. Minimum Length. The length of all system passwords shall have at least 6 characters but preferably a minimum of 8 characters. When feasible, a password shall contain a combination of letters, numbers, and symbols.
  - b. Personal Data. Personal information such as spouse's name, license plate, social security number and birthdays must not be used unless accompanied by additional unrelated characters.
  - c. Recurring Data. Users are prohibited from constructing passwords that change in a predictable or recurring manner. For example, users must not utilize passwords like AL2JAN in January, AL2FEB in February, etc.
  - d. Reuse. Users must not use passwords which are identical or substantially similar to passwords that they had previously used. In most cases, application software may prevent users from reusing a password, but may not prohibit a similar password from being used. It

is the user's responsibility to ensure a substantially different password is selected each time it is changed.

- e. Display and Printing. Displaying and/or printing passwords shall not be done. However, in rare cases when a password is required to be displayed or printed it must be screened and protected from unauthorized viewing and destroyed as soon as possible when no longer needed.
  - f. Periodic Change. All passwords shall require a mandatory change every ninety (90) days whenever possible. When feasible, network software should be programmed to accommodate and enforce this requirement.
  - g. Unauthorized Storage. Passwords must not be stored in readable form on paper, in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control or in other locations where unauthorized persons might discover them.
  - h. Suspected Disclosure. All passwords must be promptly changed if disclosure to unauthorized persons is known or suspected.
  - i. Password Sharing. Regardless of the circumstances, passwords shall not be revealed to any person other than the authorized user. Sharing with other individuals is strictly prohibited. However, in rare cases there are workstations that have multiple users and passwords are shared.
  - j. Limited Attempts. Log-on password entry shall be limited to three (3) unsuccessful attempts. The network software shall be programmed to suspend the user ID upon subsequent unsuccessful efforts to log on and shall require a System Administrator to reset the user's password.
  - k. Default Passwords. Vendor-supplied default and/or blank passwords shall be immediately identified and reset.
2. Unattended Computer Systems. Active (logged on) computer systems in use within the Department of Public Safety shall not be left unattended unless suitable measures against unauthorized viewing have been taken. This applies to all computer systems, including microcomputers (PCs), workstations, and terminal equipment.
- a. Systems can be locked by initiating a warm boot (Ctrl-Alt-Delete) and then pressing the Enter key. Employees should use their judgment on when to lock a workstation if they are away from their desk for an extended period of time especially if there is sensitive or confidential data on the machine.
  - b. If there are no means available to lock out unauthorized viewing when away from the system, the user shall log out of the system. There shall be no exceptions to this provision of the policy.

3. Unique User ID. Each computer and network system user ID must uniquely identify only one user. Shared or group user IDs are not permitted unless it is a special circumstance and must be approved by the IT/MIS Department. Each person assigned to multiple-user computer shall have a unique user ID and must log off the system before another user is allowed to sign on. If a shared computer is locked by another user who is unavailable, a forced logoff feature may be available to log a user out of the system and allow another user to log in. However, a forced logoff may close open applications, potentially resulting in the loss of unsaved data, and so should be used with caution.
4. User ID Restrictions. User IDs shall only be granted to permanent and contracted employees and consultants engaged by the Department of Public Safety. No other individual shall be granted a user ID or otherwise given privileges to use Department computer or communications systems unless authorized by appropriate management.
5. Access Termination. Supervisors shall notify the appropriate DPS representative(s) of the need for access termination. All network privileges must be promptly terminated if:
  - a. The employee no longer works for the department
  - b. The employee no longer works in a position requiring access
  - c. Access is withdrawn due to disciplinary action
6. Gaining Unauthorized Access. Employees using department information systems are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operation of other systems. Users are also prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.
7. Unauthorized Programs and Equipment. Users may not install any computer program or equipment developed or purchased outside the Department of Public Safety on their PCs, on network servers, or on computers connected to the network. Should the need arise for a unique software program or equipment component, the user shall obtain authorization from the IT/MIS section before purchasing or installing a software program. IT/MIS will authorize the purchase through Department channels if the item is deemed necessary for an official job function.
8. Suspected System Intrusion. If a user suspects that his or her computer system has been compromised in any way, the suspect computer shall be

immediately removed from all network systems. The user shall inform his or her immediate supervisor who will immediately notify the Information Security Office. IT/MIS will provide the necessary technical skills to eradicate the intrusion and restore the computer system back to its original configuration. The computer system shall not be reconnected to a network system until specifically authorized by IT/MIS.

9. Violations. Violations of this policy may result in revocation of privileges, restricted access to network systems, and/or other appropriate disciplinary action, up to and including dismissal. The Department of Public Safety reserves the right to monitor all network assets, including employee Internet usage.