ILLINOIS STATE POLICE DIRECTIVE
SRV-218, COMPUTER PASSWORD CONTROL

RESCINDS: SRV-218, 2014-056, revised 06-27-2014.	**REVISED:** 01-14-2016 **2016-004**
RELATED DOCUMENTS: None	**RELATED CALEA STANDARDS:** 82.1.6

I. POLICY

The Illinois State Police (ISP) will establish and administer a directive for microcomputer password control and violation reporting.

II. RESPONSIBILITIES

Employees are responsible for ensuring their microcomputer password is not compromised and notification of chain-of-command if they suspect their password has been compromised.

III. PROCEDURES

III.A. Temporary passwords

III.A.1. A temporary password will be created for employees when their user ID is created or reset.

III.A.2. All temporary passwords must immediately be changed following the guidelines in paragraphs III.B.2. and III.B.3.

III.B. Changing passwords

III.B.1. System software should require the changing of passwords every 35 days. Users are required to change their passwords every 35 days if the system software does not force a password change.

III.B.2. Remote Access Control Facility (RACF) passwords must be eight alphanumeric characters in length, with at least one character being alphabetic and at least one character being numeric. Users are encouraged not to use any word found in the dictionary and to incorporate special symbols (#, $, %, &) frequently. Active Directory windows passwords can be 8 to 256 characters in length, and must contain three of the following characters: alphabetic uppercase, alphabetic lowercase, numeric (0-9), and special (non-alphanumeric, .i.e., ( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /), and may not contain three or more sequential characters of your name nor contain the user's account name value or display name.

III.B.3. Obvious passwords such as nicknames, dates of birth, family members' names, or months of the year should not be used.

III.B.4. If during an emergency users must share their password, they are required to change their password as soon as reasonably possible.

III.C. Password security

III.C.1. Passwords should be handled with the strictest confidentiality.

III.C.2. Passwords should not be shared with another user, unless necessitated by an emergency situation.

III.C.3. Passwords must not be written down.

III.C.4. Passwords stored in computer memory or storage should be encrypted to prevent unauthorized disclosure.

III.C.5. The password-suppression feature will be used on all terminals to prevent the display of a password during system log-on.

III.C.6. User ID's will be disabled/revoked when the user enters an incorrect password three consecutive times.

III.C.7. Most system software maintains a history of unsuccessful password attempts and unauthorized access to systems.

III.C.7.a. RACF (mainframe) system logs are reviewed daily by security administration.
III.C.7.b. The appropriate supervisor is notified of unauthorized access attempts for verification with the user(s).

III.C.8. Most system software will maintain a history of at least 24 previous passwords for users to minimize the reuse of passwords.

III.C.9. Workstations must be locked when unattended.

III.D. Users who have forgotten their password must contact the ISP Integrated Help Desk (217/782-4155 or 1-800-532-3700) or Security Administration ("Security Security" via Lotus Notes) for their password to be reset.

III.E. Users will only be contacted at a phone number in ISP's e-mail system for resetting a password.

Indicates new or revised items.

-End of Directive-