

IDAHO STATE POLICE PROCEDURE

13.02 PASSPHRASES

I. GENERAL

Passphrases are used for authentication to allow users into the Idaho State Police (ISP) network. Passphrases must meet specific standards, be constructed according to set length, and complexity requirements.

II. DEFINITIONS

- A. "Account Disable" means a state in which an account has been administratively disabled.
- B. "Account Lock" means a state in which a user is automatically prevented from logging into the network.
- C. "Breach Corpuses" means a collection of known compromised passwords and phrases.
- D. "Passphrase" means a memorized secret consisting of a sequence of words or other text that an individual uses to authenticate their identity. A passphrase is also referred to as a password or memorized secret and is generally longer than a traditional password for added security.
- E. "User ID" means a unique identifier, commonly used to log on to a website, app, or online service. It may be a username, account number, or email address.

III. PASSPHRASE REQUIREMENTS

- A. Passphrases must:
 - 1. be a minimum of any twenty (20) characters, including spaces;
 - 2. not be a derivative of the User ID;
 - 3. not be obtained from previous breach corpuses;
 - 4. not be displayed when entered;
 - 5. not include repetitive or sequential characters;
 - 6. not be any of the previous 24 passphrases; and
 - 7. be changed:
 - a. Every 365 days; or
 - b. If prompted.

IV. ACCOUNT SECURITY

- A. Accounts:
 - 1. will lock upon passphrase expiration date;
 - 2. after five (5) consecutive failed login attempts within 15 minutes;
 - 3. will not unlock automatically after a set amount of time; and
 - 4. will be unlocked only by the Idaho Office of Information Technology Services (ITS) Service Desk after identity validation.

IDAHO STATE POLICE PROCEDURE

B. Compromised passphrase

1. Passphrases will be compared to breach corpuses.
2. If a passphrase is found on breach corpuses a notification will be sent to the user who must change their passphrase within 24 hours.
3. Failure to comply with the notification will result in the account being disabled.
4. To re-enable a disabled account
 - a. The employee must notify their supervisor; and
 - b. The supervisor or above will need to contact the ISP ITS Liaison, who will coordinate re-enabling the account with ITS.
5. If you believe that your user ID or passphrase has been compromised,
 - a. immediately report the circumstances to your supervisor; and
 - b. immediately notify the ITS Service Desk by phone in accordance with ISP Procedure [EHP 13.01 Contacting IT](#).

C. ISP network security is dependent upon users being responsible for maintaining passphrase integrity. To protect passphrases, do not:

1. divulge your passphrases to anyone;
2. save passphrases where others can find them;
3. use passphrases that are intuitive or easy to guess;
4. use the same passphrase for multiple systems;
5. use a "Remember Passphrase" feature; or
6. use hints about your passphrase's composition if prompted by any program or system.