DCIN Password Requirements & Specifications

In full compliance with the FBI CJIS Security Policy and within state network security guidelines, the SBI manages the DCI Network password structure and expiration.

Certified users are responsible for creating and managing his/her DCIN password according to the requirements below. Terminal Agency Coordinators and their assistants (TACs/ATACs) are to ensure agency compliance by all agency users for DCI Network security.

DCI Network passwords and structures should be maintained as follows:

1) Passwords shall consist of a **minimum eight (8)** character and a **maximum twelve (12)** character format. On all systems (Omnixx and mobiles), DCIN passwords must contain **at least one (1) letter, one (1) number, and at least one (1) special character**.

   a. Passwords cannot be the same as a User ID in any case.

   b. Special characters that work best with DCIN are: **! @ # $ ***

   c. Do **NOT** use any of these as a special character: period(.), forward slash(/), less than(<), underscore(_), dash(-), quote("), ampersand(&), plus sign(+), percentage(%) or curly brackets ({or}).

   d. Passwords cannot be a dictionary word or proper name.

   e. Passwords cannot be displayed when entered.

   f. Passwords cannot be transmitted in the clear outside the secure location.

2) **Passwords shall expire every ninety (90) days**.

   a. No user is exempt from this requirement. Non-expire or future set passwords are security violations. DCIN quality reviews will be conducted periodically to monitor and address password violations.

   b. Passwords cannot be re-used within fifteen (15) password changes.

c. When a user logs into Omnixx, the user will receive a prompt at least fifteen (**15**) days before the password expiration allowing the user to change the password.

d. Mobile software will notify mobile users when their passwords will expire. Agencies are encouraged to develop a policy to ensure mobile users change their passwords in a timely manner.

3) Passwords can be changed at **ANY** time at the DCI Network Log On transaction on either an Omnixx desktop or mobile device.

a. When changing passwords, more than just a couple of characters must be changed. Failing to do so will cause the user to be eventually locked out of the system.

b. After entering the old password in the "Current Password" field and new password in the "New Password" field and re-typing it in the "Confirm" field, the user clicks "OK" and receives a notification of Successful Password Change.

c. If a user does not change his/her password by the expiration date, the agency TAC/ATAC will have to reset the password individually. TACs/ATACs must use **UPPERCASE** when establishing new passwords or resetting passwords in Console.

* * * * * * * * * * * * * * *

If you have questions regarding DCIN passwords,
contact your agency TAC/ATAC.

If additional guidance is needed,
TACs/ATACs contact their SBI District Training Specialist.

* * * * * * * * * * * * * * *