

NNOOC F&SCM

Security Statement

Security and User Identification

Access to F&SCM users require a User ID and Password. Users must submit a F&SCM Security Form. Users accept responsibility for the confidentiality and security of access into the F&SCM.

Lockouts

The F&SCM uses a lock-out protocol to deter unauthorized users from repeated login attempts. The system locks the user out, requiring a phone call or email to the Department of Information Technology (DIT) or FMIS Support Department to verify the identity of the user, before resetting user's password for re-entry into the F&SCM system.

Sharing of User and Password

Users take responsibility when accessing the F&SCM system. Never share your User ID and Password with anyone, sharing your User ID and Password will result in your account being disabled for security purposes.

Protecting your user ID and Password

You should not keep your User ID and password information on or near your computer. Keep both in a secure area, away from your computer to prevent any unauthorized access to your account. Passwords must be changed through the DIT ticketing portal for initial login to the F&SCM system. Some browsers may store users ID and passwords to make it easier when you revisit F&SCM website. Navajo Nation Office of the Controller does not recommend using this feature to access the F&SCM site. You can disable this feature in your browser. Please note that if you enable this feature, unauthorized users may be able to access your account without your knowledge and could result in your account being terminated. Do not leave your computer while you are logged into the F&SCM system, especially if others may have access to your computer. Before leaving your computer, be sure to click the Sign out option to end your online session.