MILSOFT® Utility Solutions

Daffron
A Subsidiary of Milsoft Utility Solutions®

January 5, 2022

Re: CIS, FMS and WMS Report Completeness
Accuracy and Availability Confirmation
Password Policy and Administrator Access
Year-End Procedures

Daffron's Compliance Process is part of our commitment to service and quality. We periodically request confirmation from our customers that data and reporting in your Daffron CIS, FMS, and WMS systems are online and available in the production environment. Please take a moment to review the questions below:

1. Is your data within the Daffron CIS, FMS, and WMS applications available to your users?
2. While you are responsible for the completeness, accuracy and integrity of your data, are your Daffron generated reports within CIS, FMS and WMS applications complete, accurate, and available?

If the answer to both questions is yes, there is no need to respond. If the answer to either question is no, please contact Cary Hamar at cary.hamar@milsoft.com with particulars of the non-compliance issue. If we do not hear from you within 14 days of the date of this letter, we will assume compliance.

In order to ensure the security of information for our customers, we recommend a password policy. Attached is a sample password policy. This policy outlines best practices for password security, including guidelines for strong passwords and password protection standards. While a policy like this is the standard for Daffron, these practices apply to all businesses and individuals with access to sensitive and confidential information. This is also a good time to review the administrator accounts set up on your Daffron system. Employees that have level 9 authority within the Daffron security application are considered administrators. Administrator access should be provided only to employees needing that access to perform their job functions. Administrator accounts should be reviewed on a regular basis.

Year-end checklists were emailed to the main Daffron contact at your utility. These checklists should be used as a guideline to complete the year-end closing steps in certain Daffron software applications.

If you have any questions regarding this letter or any other matter, please contact me at 800.344.5647 or cary.hamar@milsoft.com.

Warm Regards,

Cary Hamar
VP Customer Service & Support

Sample Password Policy

Overview
Passwords are an important aspect of computer information security. A poorly chosen password may result in unauthorized access and/or exploitation of resources. All users, including contractors, clients, and vendors with access to Daffron systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of rotation.

Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Daffron facility, has access to the network, or stores any non-public information.

General Policy
All passwords will expire every 90 days and a new password will need to be created.

Green screen and iXp passwords must match in order for the systems to function properly. Daffron software users need to be responsible for all computer transactions that are made with his/her user ID and password.

Daffron software users should not disclose passwords. Passwords must be changed immediately if it is suspected that they may have become known to others.

- Daffron software users should not record passwords where they may be easily obtained.
- Daffron software users should log off their Daffron application sessions when leaving a workstation for an extended period of time or follow appropriate computer shut down procedures.
- Daffron software users should lock their computer whenever they move away from their workstation.

Guidelines
Daffron software users should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Must contain 6-10 characters, at least one number, no repeating characters, and the first character must be a letter.
- Passwords should not be easily guessed by others. Passwords cannot be your name, phone extension, birthdate, pet or family member name, or other easily identifiable personal information.
- After three invalid login attempts, the user profile will be disabled.