FOR SPD ACCOUNT USER

- **Do not share your password with anyone for any reason**

  Passwords should not be shared with anyone, including any family, staff, boss or anyone. Passwords should not be shared even for the purpose of computer repair.

- **Change your password periodically**

  As a general rule of thumb, changing your password every 90 days is recommended. However, you may choose to vary the frequency of password changes based on the privilege or access level of the account. Accounts of greater privilege or access level should have their password changed more frequently and vice versa. This practice prevents someone, who has obtained your password through some means, from continuing to have access to your account. **If you suspect someone has compromised your account, change your password immediately. Be sure to change your password from a computer. After resetting your password, report the incident to JPD administrator or JPD helpdesk number.**

- **Consider using a passphrase instead of a password**

  A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember. For example, the passphrase "My passw0rd is $uper str0ng!" is 28 characters long and includes alphabetic, numeric and special characters. It is also relatively easy to remember. It is important to note the placement of numeric and symbolic characters in this example as they prevent multiple words from being found in a standard dictionary. The use of blank spaces also makes a password more difficult to guess.

- **Do not write your password down or store it in an insecure manner**

  As a general rule, you should avoid writing down your password. In cases where it is necessary to write down a password, that password should be stored in a secure location and properly destroyed when no longer needed. Using a password manager to store your passwords is not recommended unless the password manager leverages strong encryption and requires authentication prior to use.

- **Avoid reusing a password**

  When changing an account password, you should avoid reusing a previous password. If a user account was previously compromised, either knowingly or unknowingly, reusing a password could allow that user account to, once again, become compromised. Similarly, if a password was shared for some reason, reusing that password could allow someone unauthorized access to your account.

- **Avoid using the same password for multiple accounts**

  While using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect allowing an attacker to gain unauthorized access to multiple systems. This is particularly important when dealing with more sensitive accounts. These passwords should differ from the password you use for instant messaging, webmail and other web-based accounts.

- **Do not use automatic logon functionality**

  Using automatic logon functionality negates much of the value of using a password. If a malicious user is able to gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.

The following are Guidelines for individuals responsible for provisioning and support of user accounts:

- **Enforce strong passwords**

  Many systems and applications include functionality that prevents a user from setting a password that does not meet certain criteria. Functionality such as this should be leveraged to ensure only Strong Passwords are being set.

- **Require periodic password changes**

  Forcing a periodic password change serves as a reminder to users and eliminates the human factor in determining whether to change a password. A general rule of thumb is to force a password change every 90 days.

- **Require a change of initial or "first-time" passwords**

  Forcing a user to change their initial password helps ensure that only that user knows his or her password. Depending on what process is being used to create and distribute the password to the user, this practice can also help mitigate the risk of the initial password being guessed or intercepted during transmission to the user. This guidance also applies to situations where a password must be manually reset.

- **Force expiration of initial or "first-time" passwords**

  In certain situations, a user may be issued a new account and not access that account for a period of time. As mentioned previously, initial passwords have a higher risk of being guessed or intercepted depending on what process is being used to create and distribute passwords. Forcing an initial password to expire after a period of time (e.g. 72 hours) helps mitigate this risk. This may also be a sign that the account is not necessary.

- **Do not use Restricted data for initial or "first-time" passwords**

  Restricted data in its data classification scheme. Restricted data includes, but is not limited to, social security number, name, date of birth, etc. This type of data should not be used wholly or in part to formulate an initial password.