PERSONNEL POLICY

Policy Number	Policy Title
4.18.1	Usernames & Passwords
Policy Source	
Information Technology Services Division	

Issued:	Revised:	Effective:
04/19/2021	04/06/2020	05/01/2021

PURPOSE

In order to ensure data security, the City of Oak Creek (hereinafter "City") provides its employees usernames and passwords for technology systems and software.

For the purposes of this policy, the term "Supervisor" shall mean the responsible Department Director or Division Manager.

The Term "Employee" shall mean any employee, appointed and elected office holder, contractor, and volunteer.

PROCEDURE

Due to the City's commitment to computer data security, the City may establish various levels of computer security for access to computer data files. All employees will be held personally accountable for all activities logged to their user accounts. Employees shall log out of or password protect any network system or work station whenever they are not using that particular program or piece of equipment. Individual departments/divisions may adopt more stringent standards based on the Supervisor's requirements and/or state and federal requirements.

A. Usernames

The standard convention for usernames is first initial last name. The only exception to this standard is in the instance of a duplicate username, at which point the convention for the new employee would be first initial middle initial last name. In the event that username already exists on City systems, the naming convention shall be first initial second letter of first name middle initial last name.

B. Passwords

A password is a string of characters used to verify the identity of a user during the logon or authentication process. Passwords are typically used in combination with a username; they are designed to be known only to the user and allow that user to gain access to a device, application or website.

1. Password Complexity

All City accounts shall be protected with a password that, at a minimum, has the following complexity:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters

- Be a minimum length of eight (8) characters;
- Contain a minimum of three (3) of the following four (4) categories:
    - English uppercase letter (A through Z);
    - English lowercase letter (a through z);
    - Base 10 digits or number (0 through 9);
    - Non-alphanumeric character (for example ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/).

This password convention must be followed for any accounts created online for City business as well. Passwords must not be reused for multiple online accounts in case of a data breach of those online services.

In some cases, various departments/divisions may have to exceed this password complexity requirement due to the data they have access to, including but not limited to Criminal Justice Information Services (CJIS) and Health Insurance Portability and Accountability Act (HIPAA) data and information.

2. **Password Age**
   City network passwords are required to be changed every 90 days. Passwords created for online accounts pertaining to City business should be changed frequently and checked for data breaches from online service providers.

3. **Password History**
   The reuse of previous passwords that have been used in the last 2 years is not recommended and blocked from City systems.

4. **Sharing Password**
   Any unauthorized sharing or disclosure of City account password(s) is a breach of security and a violation of this policy. This applies to both the employee who reveals the password and to any employee who uses it.

   The IT Services Division will never ask for your network password. If the IT Services Division needs access to your network account the password will be reset and provided to you to change.

C. Personal Identification Number (PIN)

A personal identification number (PIN) is a security code for verifying your identity. Similar to a password, your PIN must be kept secret because it allows access to City data, Servers, and Applications. PINs are most frequently used on mobile devices.

1. **PIN Security**
   Because PINs often protect City data, information and resource, a PIN that is difficult to guess must be used. Avoid including the following items in your PIN:

   - Simple number sequences like 1234 or 0000 (including repetition: 1122 or 2233)
   - Significant dates, such as birth years or birthdays
   - Any part of your Social Security Number
   - Any part of your address or phone number

Longer PINs are safer than shorter PINs. If you use a four-digit PIN, there are 10,000 possible variations (starting with 0000, 0001, 0002, and so on). With a six-digit PIN, there are 1 million possible codes. Longer PINs work better because it takes more attempts to guess them.

D. Device Security

Any device that contains or has access to City data, servers, or applications must be secured by a username/password combination or PIN. The device must also be configured to automatically wipe the device if the wrong PIN is entered more than 3 times. The City is not responsible for any data that is not backed up from the device if a wipe of the device occurs due to failed entry attempts.

E. Non-IT Managed Services Used for City Business

A Non-IT Managed Service is any service for which the IT Services Division does not have the capability to reset login information. This can be a shared account, online service account, cloud services, or internet account. For example, non-business AppleIDs, Social Media Logins, and Cloud Applications.

All Non-IT Managed Services used for City business and a list of all employees that have access to said service and their associated access level shall be filed with the Supervisor and IT Services Division.

Whenever requested, employees are required to cooperate with and to aid the City with gaining access to Non-IT Managed Services used for City business. The process to create new accounts for any Non-IT Managed Services shall be documented and on file with the Supervisor and IT Services Division.

Any Non-IT Managed services used for any City business are the property of the City and, thus, failure to cooperate with the City with gaining or restoring access to Non-IT Managed services may subject the employee to discipline up to and including termination as well as the pursuit of criminal or civil liability.

POLICY VIOLATIONS

Employees who do not adhere to this policy may be disciplined, which can include restriction of use, confiscation of device, or discipline up to and including termination or removal from office. Severe violations of this policy may also subject an employee to civil liability and criminal prosecution.

QUESTIONS

Contact the IT Services Division, your Supervisor, and/or Human Resources Manager for questions regarding anything in this policy.

EXCEPTIONS

Departments/Divisions may require special exceptions to this policy for operational, regulatory, legal, or other special requirements. The reason and process for exceptions must be documented in department/division policy and approved by the IT Services Manager.