GENERAL ORDER

MINOCQUA POLICE DEPARTMENT

SUBJECT: **PASSWORDS**

SCOPE: All Department Personnel
DISTRIBUTION: General Orders Manual

REFERENCE: WI State Statutes: 165.83, 165.84
TIME Operator Manual,
TIME System Security Manual

NUMBER: 10.07
ISSUED: 04/23/2020
EFFECTIVE: 05/03/2020
☐ RESCINDS
☐ AMENDS
WILEAG 5TH EDITION
STANDARDS: N/A

INDEX AS:
CIB System Procedures
Password Construction Guidelines
Teletype System Procedures
TIME System

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 change. The secondary purpose of this policy is to have a process in place to manage current user passwords and restrict access to prior employees.

This General Order consists of the following numbered sections:

I. POLICY

A. Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Minocqua Police Department's resources. It is the policy of the Minocqua Police Department that all users, including contractors and vendors with access to Minocqua Police Department systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

B. 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 Minocqua Police Department office, has access to the Minocqua Police Department network, or stores any non-public Minocqua Police Department information.

II. PASSWORD CREATION

A. All user-level and system-level passwords must conform to the Password Construction Guidelines.

1. All passwords must be a minimum length of eight (8) characters on all systems.

2. All passwords shall not be a dictionary word or proper name.

B. Users must not use the same password for Minocqua Police Department accounts as for other non-Minocqua Police Department access (for example, personal ISP account, option trading, benefits, and so on).

C. Where possible, users must not use the same password for various Minocqua Police Department access needs.

D. User accounts that have system-level privileges granted through group memberships or programs such as Active Directory must have a unique password from all other accounts held by that user to access system-level privileges.

E. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

III. PASSWORD CHANGE

A. All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a 90 day basis.

B. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every 90 days.

1. Passwords must not be identical to the previous ten (10) passwords.

C. Password cracking or guessing may be performed on a periodic or random basis by the Technology Management team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

IV. PASSWORD PROTECTION

A. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential, Minocqua Police Department information.

B. Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.

    1. Passwords must not be transmitted in the clear outside the secure location.

C. Passwords must not be revealed over the phone to anyone.

D. Do not reveal a password on questionnaires or security forms.

E. Passwords must not be displayed when entered.

F. Do not hint at the format of a password (for example, "my family name").

G. Do not share Minocqua Police Department passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

H. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

I. Do not use the "Remember Password" feature of applications (for example, web browsers).

J. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

V. APPLICATION DEVELOPMENT

A. Application developers must ensure that their programs contain the following security precautions:

    1. Applications must support authentication of individual users, not groups.

    2. Applications must not store passwords in clear text or in any easily reversible form.

    3. Applications must not transmit passwords in clear text over the network.

    4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

VI. MANAGEMENT OF USER PASSWORDS

A. All user passwords are to be created in Active Directory by an authorized administrator of the network (Department's delegated IT Agent/Technology Management), and then changed by the users according to policy requirements. Any unauthorized access to the server Active Directory resides on is prohibited.

VII. RESTRICTING ACCESS TO PRIOR EMPLOYEES

A. If an employee of Minocqua Police Department is terminated or leaves their position the following actions will take place:

    1. Access to any network rights on the Minocqua Police Department's network will be removed.

    2. Any remote access the employee has to the Minocqua Police Department's network will be removed.

    3. Passwords will be changed for all applications the employee had access to on the network or

their computer.

4. The employee's user account will be removed or disabled in Active Directory.

VIII. POLICY COMPLIANCE

A. Compliance Measurement

1. Technology Management will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

B. Exceptions

1. Any exception to the policy must be approved by the Chief of Police in advance. After conferring with the Department's designated IT agent, the Chief of Police will determine if the exception is approved.

C. Non-Compliance

1. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

David J Jaeger

David J. Jaeger
Chief of Police

This General Order cancels and supersedes any and all written directives relative to the subject matter contained herein.

Initial 10/26/2017