Sheridan Police Department
Policies and Procedures
15.2
Chapter 15 – Information Systems
Section 2 – Department Information Systems

Date: January 1, 2013
Updated: 7/23/2021

Signature:

The department provides computers, cell phones, electronic mail, voice mail, mobile data terminals, and access to the internet to enhance productivity and effectiveness.

15.2.1 Information System Policy References

A. The City of Sheridan Information Technology Division is responsible for the maintenance and control of the department's various computer equipment, software and related peripherals.

B. The acceptable use policy is contained in City of Sheridan Employee Handbook .
   1. Use of the department's computers is limited to purposes directly related to the mission of the department
   2. Employees do not have a reasonable expectation of privacy when using any department-owned computer equipment.

C. E-mail use is governed by City of Sheridan Handbook and law.
   1. Transmission of electronic messages and data will be conducted with propriety and professionalism.
   2. Obscenity, threats of violence and harassment are all prohibited.

D. The security of records, data, hardware, software, networks and systems is governed by City of Sheridan.
   1. For security reasons, employees should not leave an active computer session unattended.
   2. Employees shall not add passwords to files or folders stored on department computers.

E. The internet access and use policy is contained in City of Sheridan Employee Handbook.

F. Voice mail usage is governed by the City of Sheridan.

G. The City of Sheridan IT Department implemented the usage of authenticators to access City-owned computers and information systems. The authenticator shall be used every time an employee logs into a City-owned information system, first by entering in their unique log-in credentials. One of the following procedures will be implemented at the City of Sheridan IT Manager's discretion:

   1. Soft Token authentication: The system will send a "push-notification" to the employee's personally-owned cell phone to verify the attempted log-in.

   2. Soft Token authentication: The system will prompt the user to enter a one-time password (OTP) PIN with the following requirements:
      a. Be a minimum of six (6) randomly generated characters
      b. Be valid for a single session

c. If not used, expire within a maximum of five (5) minutes after issuance.

3. Hard Token authentication: City of Sheridan IT Manager will issue a hard-token for the employee utilize for logging into the City-owned systems.