COVINGTON POLICE DEPARTMENT
STANDARD OPERATING PROCEDURE

Subject: USE OF COMPUTERS	
Date of Issue: 05-22-2012	**Number of Pages: 5**
Policy No. A255	**Review Date:**
Distribution: All	**Revision Date: 11-30-2017**

I. Purpose

To establish strict procedures for the usage of all department issued laptops and desktops and to ensure that the computer resources are used properly by the employees.

II. Statement of Policy

The Covington Police Department relies on its computer network, standalone PC's, and laptops to conduct its business.

The rules, procedures and obligations described in this policy apply to all Users (referred to as the "Users") of the Covington Police Department's computer network, wherever they may be located. Violations will be taken very seriously and may result in disciplinary action, up to and including termination, and civil and/or criminal liability.

Therefore, it shall be the policy of the Covington Police Department that it is every employee's duty to use the department's computer resources responsibly, professionally, ethically, and lawfully.

III. Definitions

1. **Computer resources** − refers to the Covington Police Department's entire computer network. Specifically, computer resources includes, but are not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, software, data files, internet connections, and all internal and external computer and communications networks (for example, Internet, commercial online services, value-added networks, e-mail systems) that may be accessed directly or indirectly from the department's computer network.

2. **Users** − refers to all employees, temporary workers, and other persons or entities that use our Computer resources.

IV. Procedures

The computer resources are the property of the Covington Police Department and may be used only for departmental purposes. Users are permitted access to the computer resources to assist them in performance of their jobs. The department requires that each

employee has access to the network, applications, and/or NCIC/GCIC for the purpose of storing, processing, and/or transmitting information. Each user shall be uniquely identified by the use of a unique identifier (user account and password). A unique identifier shall also be required for all persons who administer and maintain the system(s) that access agency and NCIC/GCIC information and/or network. Use of the computer system is a privilege that may be revoked at any time. The department requires each user to identify themselves on the system before the user is allowed to perform any action on the network or its applications. Active directory passwords (user accounts are changed every 180 days. All user IDs shall belong to currently authorized Users only. Employees shall not share their IDs with other employees, supervisors, management, family members, or friends at any time.

In using or accessing our computer resources, Users must comply with the following provisions:

A. No Expectation of Privacy

1. ***No expectation of privacy.*** The computers and computer accounts given to Users are to assist them in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the Covington Police Department and may be used for department business only. The Covington Police Department can monitor its computers for compliance and might "inspect all files and messages at any time."

2. ***Waiver of privacy rights***. Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Users consent to allowing authorized personnel of the Covington Police Department to access and review all materials Users create, store, send, or receive on the computer or through the Internet or any other computer network that is department owned. Users understand that the department may use human or automated means to monitor use of its Computer resources.

B. Prohibited Activities

1. ***Inappropriate or unlawful material.*** Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent or received by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in the city's computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

2. ***Prohibited uses***. Without prior written permission from the Chief of Police or his designee/s, the department's computer resources may not be used for dissemination or storage of commercial advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political material, or any other unauthorized use. This includes using Covington Police Department's email address lists to propagate personal information.

3. ***Waste of computer resources.*** Users may not deliberately perform acts that waste Computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.

4. ***Misuse of software.*** Without prior written authorization from the information systems specialist, Users may not do any of the following:

   a. copy software for use on their home computers.

   b. provide copies of software to any independent contractors or agents of the department or to any third person.

   c. install software on any of the department's workstations, servers, standalone pc's, or laptops.

   d. download any software from the Internet or other online service to any of the department's workstations, servers, standalone pc's, or laptops.

   e. modify, revise, transform, recast, or adapt any software.

   f. reverse-engineer disassemble, or decompile any software. Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

5. ***Communication of protected information.*** Unless expressly authorized by the Chief of Police, sending, transmitting, or otherwise disseminating proprietary data or other confidential information of the department is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties.

C. Passwords

1. ***Responsibility for passwords.*** Users are responsible for safeguarding their unique passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system with another user's password or account.

2. ***Passwords do not imply privacy***. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. The Department has global passwords that permit it access to all material stored on its computer system-regardless of whether that material has been encoded with a particular user's password.

D. Security

1. ***Accessing other user's files.*** Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another user does not imply permission to read, alter or copy that file. Users may not use the computer system to 'snoop" or pry into the affairs of other Users by unnecessarily reviewing their files and e-mail.

2. ***Accessing other computers and networks***. A user's ability to connect to other computer systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

3. ***Computer security***. Each user is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of the department's computer resources. This duty includes taking reasonable precautions to prevent intruders from accessing the Department's network without authorization and to prevent introduction and spread of viruses.

4. Removal of Users. Active directory (user accounts) shall be disabled upon termination of employment by the Information Systems Manager. The Information Systems manager is also responsible for making the Spillman administrator aware of the employee's departure from the police department so that they could be removed from Spillman. The Information Systems Manager shall also be responsible for notifying the TAC of an employee's departure so the employee can be removed from GCIC.

E. Viruses

1. ***Virus detection.*** Viruses can cause substantial damage to computer systems. Each user is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the department's network. To that end, all material received on usb thumb drives, electronic media, or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to the department **MUST** be scanned for viruses and other

destructive programs before being placed onto the computer system. Users should understand that their home computers and laptops may contain viruses. All disks transferred from these computers to the department's network **MUST** be scanned for viruses by the department's information systems specialist.

2. ***Accessing the Internet.*** To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to the department's network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited unless the computer you are using is not connected to the department's network.

F. Encryption software

1. ***Use of encryption software.*** Users may not install or use encryption software on any of the department's computers without first obtaining written permission from the Information Systems Specialist. Users may not use passwords, encryption keys, key loggers, or similar applications that are unknown to their supervisors and/or the systems information specialist.

G. Miscellaneous

1. ***Compliance with applicable laws and licenses.*** In their use of computer resources, Users must comply with all software licenses; copyrights; and all other state, federal, and international laws governing intellectual property and online activities.
2. ***Electronic Medias shall be disposed of when required.*** One of the following three ways will be used: Overwriting, degaussing, or destruction. IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from the Covington Police Department's control until the equipment has been sanitized an all stored information has been cleared using one of the above methods.

3. ***Other policies applicable.*** In their use of computer resources, Users must observe and comply with all other policies and guidelines of the department.

4. ***Amendments and revisions.*** This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

5. ***No additional rights.*** This policy is not intended to, and does not grant Users any contractual rights.

This SOP supersedes any SOP previously issued.

BY ORDER OF THE CHIEF OF POLICE:

Stacey L. Cotton

Stacey L. Cotton
Chief of Police