DOUGLAS COUNTY SHERIFF'S OFFICE		Policy and Procedure
Specific Policies **Use of Communication Technologies**		**P&P-B-119**
Effective Date: 02-26-20 Supersedes: 12-02-15	Approval: Sheriff	Number of Pages: 3
References:	Reevaluation Date: Annually	Standards: CALEA LE 11.4.4, LE 41.3.7 COM 1.2.2, 6.8.3, 6.8.4, 6.8.7, 6.8.5

I. POLICY

Telecommunication and computer technology is rapidly evolving. This Office recognizes the need to make these technologies available to our employees and authorized users of specific software. The ability to access information services is an essential job requirement. These services include records management systems, New World Systems, NCIC, Colorado State Courts Data Access, the Internet and Intranet, and telecommunications devices such as pagers, telephones, mobile data computers, and other electronic devices.

II. PROCEDURE

Data stored on these systems is to be used within the parameters of the member's job assignment. <COM6.8.4d> Certain federal or state statutes may regulate and restrict the access, release, and use of this data. Violation of law may include criminal charges and or civil sanctions.

Use of this information for other than professional purposes, EX: assisting unauthorized persons to obtain or access information, or releasing information to unauthorized persons are grounds for removal of access and/or discipline, up to and including termination. <COM6.8.4e>

Improper use of telecommunication devices is also prohibited. Use of telecommunication devices, e-mail, and other county-owned messaging systems for personal messages should not be abused. <COM6.8.4e>

E-mail transmissions and Internet Usage files and logs are subject to review by internal staff at any time and may be subject to public access under the Public Records Act. Files stored on local, network or removable drives are open for inspection at any time. There is no expectation of privacy on any Sheriff/county-owned electronic device to include but not limited to cell phones, smart phones, pagers, tablets or other network appliances and computers.

The Sheriff's Technology Manager directs their staff to conduct a monthly audit of at least one random Sheriff's Office computer and one random computer used in the communications center. All supervisors in the Sheriff's Office are responsible to review the electronic transmissions of their assigned subordinate employees. This can be accomplished by keeping aware of what is on your subordinate's monitors. If the supervisors notice misuse by a subordinate, the Sheriff's Office Technology staff should be contacted to complete an audit of that computer. <COM1.2.2> <COM6.8.4c> <COM6.8.4f> <COM6.8.5> <LE 41.3.7>

Multi-Factor Authentication (MFA) is a method to increase security of mobile devices or remote access from outside the Sheriff's Office/County network, (I.E. laptops, cell phones, or other "off network" devices. In order to use MFA, users will need to have

Microsoft Authenticator installed and configured on a device to allow the MFA notification. This includes any office issued cell phone, (including s"tipend" phones) or personal cell phone. Without this authentication, remote access to most Office resources will be blocked.

Official Sheriff's Office member email signatures shall be written in English and contain rank/title, first and last name as well as relevant business contact information. Email signatures may also contain the Sheriff's Office web address and official Sheriff's Office social media links. Members may also attach the official Sheriff's Office badge or patch to their signature. Quotes, slogans, phrases or images other than those officially sanctioned by the Douglas County Sheriff's Office are prohibited.

The Internet is a powerful way to access information but is not without risk. Despite the use of software to limit access to certain sites, users of the Internet might encounter inappropriate material or contact undesirable people when communicating. Supervisors should stay aware and if they notice inappropriate material of electronic transmissions they should notify Sheriff's Technology staff.<COM6.8.4a><LE 41.3.7>

Users may not install or download programs, drivers, screen savers, or demonstration software without authorization from the Sheriff's Office technical support staff. <LE 41.3.7a><COM 6.8.3> Many of these contain malicious programs or viruses that can place the network and information at risk. <COM6.8.4b> E-mail messages with unknown attachments should not be executed or opened. Users may not modify or manipulate any software function beyond its intended use. <LE 41.3.7b> <COM 6.8.3><COM6.8.4e>

In order to ensure that contemplated technology purchases are compatible with and will interface correctly with existing and future systems, all technology and telecommunications-related purchases must be approved by the Sheriff's Technology Services manager. This includes, but is not limited to software, computers, printers, fax machines, scanners, telephones, Smart phones, tablets, etc. <LE 11.4.4>

Regardless of funding source, all technology belonging to the Sheriff's Office that connects to the Sheriff's Office data systems or networks will reside on a designated domain and will be managed by Sheriff's Office Technology Services. All devices that connect to the production domain will be loaded and managed by Information Technology Services before being connected to the network. This includes the device joining the production domain, having antivirus software installed, and running any workstation management tools or agents necessary for computer management and administration.

Any outside connection to Sheriff's office infrastructure, (servers, workstations, applications databases, etc.) must be reviewed and approved by the Technology Services manager.

All contracts related to technology must be reviewed and approved by the Technology Services manager and the Support Services Division Commander.

The Internet should be used for purposes directly related to the performance of the job function.

III. PASSWORD ACCESS AND SECURITY

Security is performed by our Windows Domain, and/or security provided by the application. We follow CJIS security standards for computer/application access. These standards are enforced by active directory/application policy and cannot be modified by end users.

In reference to CJIS Security policy; 5.6.2.1 Standard Authentication (Password)

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall: <LE 6.8.7a>

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. The password must include 3 of the following criteria:
   a. Upper Case letter
   b. Lower Case letter
   c. Number
   d. Special Character (IE: !@#$%^&*()<>)
4. Not be the same as the User ID.
5. Expire within a maximum of 90 calendar days. <LE 6.8.7b>
6. Not be identical to the previous ten (10) passwords.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.
9. Once changed the user's password cannot be changed again for 7 days.

Passwords and access codes should be considered confidential information.

Tech services is responsible for password access termination when employment status or position changes. <LE 6.8.7c>

IV. VIOLATIONS OF DEPARTMENT POLICY

No employee will;

A. Deliberately seek out, display, or create material that could be offensive to anyone. This includes, but is not limited to, material that is racist, sexist, homophobic, pornographic, religious, irreligious, or which contains abusive language.

B. Harass, insult, or attack others.

C. Intentionally damage computer equipment, systems, or networks or their data, or run programs to unnecessarily consume resources or deny access.

D. Share passwords or use programs to capture authorization codes or passwords.

E. Violate copyright laws by copying or redistributing copyrighted materials.

F. Use another person's passwords or access codes.

G. Obtain unauthorized access to accounts, files or data on any computer or network.

H. Assist other people, inside or outside the county, to obtain unauthorized access to information held within the county's systems.

I. Intentionally waste computer resources.

J. Utilize the county network or computers to access or post on social networking sites for personal use.

K. Absent an emergency, no employee will use a mobile communication device (mobile phone, cell phone) while driving a county vehicle unless also using that mobile device in a hands-free mode, i.e., using an earpiece, speaker phone, etc.

L. No employee will use mobile communication devices, to also include a pager or MDT, for purposes of writing CAD notes, reports, or sending text or chat messages while driving a county vehicle, unless the vehicle is stopped.

V. VIOLATION OF POLICY / PROCEDURE

Violation of any of these policies or procedures may result in any or all of the following:

A. Removal or restriction of access to systems. (Access to communication technologies is part of the essential job function. Removal or restriction would impair your ability to perform those essential functions).

B. Internal discipline, up to and including termination.

C. Criminal charges and/or civil sanctions.

D. Other sanctions that are within the scope of the organization and appropriate to the situation.

By Order of the Sheriff