CHAPTER:	1	Administration and Management	**1. 1. 22**
SECTION:	1	General Administration	**EFFECTIVE DATE: 03 / 09 / 2020**
SUBJECT:	22	**COMPUTERS AND COMMUNICATION RESOURCES**	
STANDARDS: ACA – 4 – ALDF: 7D-17, 7D-22			
APPROVED: _____ **Dale Glass** **COMMISSIONER OF CORRECTIONS**			**REVISION DATE:** 3 / 8 / 21 **REVISION DATE: 3 / 23 / 21**
Rescind: 1.1.22 dated 4/13/20 Cancel:			

I. POLICY

It is the policy of the St. Louis City Division of Corrections to provide computers, computer software, and other communication related resources and equipment for use by Divisional employees for administrative and business-related purposes, and to protect against any unauthorized use of, or access to, or routine viewing of Divisional computer devices, access devices, and printed and stored data.

II. PURPOSE

To define the boundaries of acceptable use of Division of Corrections computers, and communication resources, including computer software, networks, electronic mail services, electronic information sources, voice mail, telephone services, and other communication resources.

III. RESPONSIBILITIES

All Division of Corrections staff, contractors, volunteers and inmates are responsible for adhering to the following procedures.

IV. DEFINITIONS

Criminal Justice Information Systems (CJIS): Federal agency responsible for establishing the level of Information Technology security requirements determined acceptable for transmission, processing and storage of the nation's criminal justice data.

Computer Peripherals: Any equipment that can be attached to a computer. Peripherals include, but not limited to printers, scanners, digital cameras, diskettes, etc.

Disks: Computer disks including zip disks and compact disks (CD's) etc., which can be used to transfer programs from computer to computer.
Emergency Request: Requests for equipment, services or repairs that impact significantly on facility operations and/or involve relocating of equipment.
"F" Drive: A subsection of the hard drive designated for personal use i.e. personal business-related correspondence and or documents such as Employee Action Reports, completed Incident Reports, memorandums and completed Disciplinary Reports.

FAMS (Fixed Asset Management System): A listing of all Division equipment valued at $500 or more.

G-Mail: The official collaboration/e-mail software in use by the Division and managed by the City of St. Louis Information Technology (IT) Services Division.

"H" or (Share) Drive: A subsection of the hard drive designated for all Division of Corrections employees; i.e. management logs, templates, blank forms and other shared documents.

Integrated Jail Management System (IJMS): Automated jail management system used by the Division of Corrections.

Internet: The global collective of computer networks. The Division's Internet access is administered by the City of St. Louis.

ITSA (Information Technology Service Agency): The City agency responsible for maintaining and monitoring the City's computer networks.

IT Coordinator (Divisional): Designated Divisional staff responsible for maintaining interdepartmental operation of agency specific applications on work stations. This person coordinates requests for computer training; computer repairs/ troubles-hooting; initial support to end users access and ensures compliance with ITSA Network Systems Policy

Non-emergency Request: Requests for information technology services that do not impact significantly on Divisional operations and/or does not involve relocating of equipment.

REJIS: Regional Justice Information System is an information service agency that provides automated access to local, state, and federal criminal justice data including, but not limited to, arrest, criminal history, want, warrants, corrections and court files.

User ID: For the purpose of this policy refers to log-on ID, log-in ID, User ID, or any other term used to describe a user's right and privileges on a computer, computer system or network.

V. GENERAL INFORMATION

1. The St. Louis City Division of Corrections computers and communication resources are the property of the City of St. Louis.

2. The Division of Corrections retains the right, and will exercise the right through its authorized personnel, to inspect and review any user's computer, data, files, notes and other information contained in it, and any data sent or received by that computer when reasonable and in pursuit of legitimate needs for supervision, control and efficient operation of the work place.

3. For the inspection and/or a review of any user's computer "F-Drive," the authorized personnel (i.e., the Divisional IT coordinator), will consult and obtain written approval from the Commissioner/designee prior to such action. The written approval and a copy of the inspection or review result will be submitted to the Commissioner of Corrections/designee, and a copy is filed by the Divisional IT coordinator.

4. Any order of the Court, or requests from any federal or state criminal agency, or the city ITSA to conduct inspection or review of Divisional computer usage by any employee, for alleged abuse or criminal violation, will be directed to the Commissioner of Corrections for implementation.

5. Computers and Communication systems obtained by any Division of Corrections facility or unit shall follow these general guidelines:

    a. The hardware shall allow for the incorporation of additional features.

    b. The software shall allow for development of new applications.

    c. The systems shall have the ability to interact with city, state and federal information systems, provided that appropriate standards and communication protocols are complied with.

    d. All proposed computer or communication system purchases will provide some or all of these general guidelines. If applicable an official waiver shall be requested from the Commissioner. The waiver request shall include a description of the following:

        1) The computer and communication hardware, software requirements and specifications.

2) How it meets the general guidelines,

3) What general guidelines it does not meet,

4) A justification regarding its need and purpose,

5) What will happen if it is not approved.

6) How staff will be trained to use it.

6. The Division or departments shall only purchase or acquire computers and communication resources hardware, software or related technologies that are officially recognized in compliance with the City of St. Louis' ITSA.

7. When staff's affiliation with the Division of Corrections terminates, the Division will terminate access to computers, communications resources and accounts. The employee must return all Divisional issued personal computers and related equipment to the IT Coordinator for inspection and inventory before the final employment check can be released.

8. Most electronic information produced in the course of city business is considered a public record. All electronic information gathered utilizing city equipment remains the property of the Division of Corrections.

9. Confidentiality of e-mail and other network transmissions cannot be assured. All staff should exercise caution when sending confidential or sensitive information by e-mail or over the network.

10. Access to the Division's computers and communication resources is regulated by this policy, the City of St. Louis ITSA policies, and in part by CJIS (see Procedure B, item #3).

11. Division employees may be granted access to the system and its applications, dependent on job assignment and authorization by the Appointing authority/designee.

12. With the exception of Housing Unit Management Logs, employees must not save any confidential, personnel or other restricted documents to the "H" Drive. (The "H" Drive is a common drive that all DOC authorized computer users have access. Confidential or restricted documents placed or created on the "H" Drive can be viewed by anyone).

13. The Division retains the right through its authorized staff member(s), to remote into any folder, briefcase or documents and their contents as found in Division's

H/drive in pursuit of conformity with this procedure and work rule and without notice to users.

14. The Divisional IT Coordinator is responsible for implementing and monitoring of this policy.

15. All Division's employees, contractors, volunteers and inmates who have access or seek access to the Division of Corrections computers will sign a consent form indicating that they have knowledge of the Division's policies and procedures in regards to the use of the Division's computing resources and the Division's policy on confidentiality and will meet the requirements established.

VI. PROCEDURE

A. Acquisition of Computers and Communication Systems Hardware, Software and/or Related Resources.

1. All computers and communication systems hardware, software or related resources will be purchased or acquired in coordination with the Divisional IT Coordinator.

2. All requests for the purchase, acquisition and installation of computers and communication resources equipment, including printers, must be submitted in writing to the IT Coordinator review.

B. User Access and Security of System

1. Staff Authorized Access;

   a. The Division will provide initial access to personnel, dependent on their job assignment, to the appropriate computer system maintained by the Division.

   b. Any request for access, and/or services or repairs to, Divisional Computers and Communication resources by employees will be made on DOC Form #1.1.22-D and forwarded to the Divisional IT coordinator in accordance with the provisions of this policy.

   c. Employees will submit completed request form to their supervisors who co-signs the request and forwards the request to Divisional I.T. Coordinator.

   d. The Divisional I.T. Coordinator reviews the request and obtains final authorization from the Appointing authority/designee prior to final action.

   e. Each employee will be required to determine a password for their personal log-on.

f. Staff member shall not solicit another staff member's password or offer their own.

g. The Internal Affairs Unit shall fully investigate any alleged inappropriate use and submits a report to the Detention Center Superintendent.

2. Inmate Access

a. Inmates are not allowed under any condition to utilize the computers designated for staff use.

b. All Division's computers and related equipment shall be clearly marked and indicated on FAMS Report.

c. Inmates may be allowed to use computer disks or other peripherals such as printers, scanners, digital cameras, etc., for appropriate work related assignments and educational programs under authorized supervision, and on computers designated for inmate use.

3. Security of System (see CJIS-ITS-DOC-08140-4.5)

a. All visitors or maintenance contractors requesting access to computer areas shall be escorted by authorized personnel at all times. The escorting person shall remain on site while the contractor performs and concludes the repair.

b. Divisional employees who have authorization to access information from restricted criminal justice information sources are subjected to national fingerprint-based record check to qualify for access to computers.

c. Divisional employees may not utilize the St. Louis Metropolitan Police Department's computers and other related equipment from the Police supervisor or designee.

d. All Non-Divisional employees will declare in writing (See DOC Form #1.1.22 - 2) to the Commissioner/designee what information computer technology system hardware, software, or related equipment they intend to introduce and, for what purpose. Inmate will have access. This form must be submitted to the Divisional I.T. Coordinator who reviews, recommends and forwards the request to the Appointing authority/designee for final approval.

e. The Divisional IT Coordinator will, at the direction of the Commissioner of Corrections/designee, coordinate and maintain a comprehensive plan in the event of a disaster, disorder, or emergency.

4. Passwords

a. Passwords are used to prevent unauthorized personnel from accessing the Division's computer and communication resources.

b. Passwords will not be written down where they can be found by unauthorized personnel and must not be shared with other individuals. No staff member will work under another's password.

c. If a user forgot their password, they should contact the Area Supervisor. The area Supervisor will contact the Divisional IT Coordinator for password resets. During normal business hours the Divisional IT Coordinator can be contacted by phone or via e-mail.

C. Logging-On and Off the Computer

1. Logging-On

a. All employees with Divisional authorized computer user access are required to log-on at the beginning of their work shift with their personal login password.

b. Users must properly log-on and off the network

c. Users must not bypass normal log-on procedures

d. Users must always use their employee's User ID and password.

e. Users must have only one simultaneous connection to the network.

f Users must verify that the username that appear in the dialog box is their username. The Dialog Box often retains the previous user's information.

g Users must read and acknowledge any error message that appears and:

2. Logging Off

a. Save all running programs before logging off

b. Users in secure areas or with access to sensitive information must always log off their system or lock their workstation before leaving their computers unattended.

D. Division's Shared Drive - H/Drive

1. The Division's shared drive is part of the electronic data and information depository sites of the Division. Access to this site is open to all Divisional staff.

2. Only items of general relevant information necessary for the general operation of the Division's job functions may be placed and saved in the H/Drive. Examples of items which may be saved in the H/Drive are:

a. Shifts' blank forms or templates.

b. Division's policies and procedures.

c. Division's blank forms or templates.

d. Housing Units' blank forms or templates.

e. Volunteer program.

f. Caseworkers' blank forms or templates.

g. Business Office operation forms or templates

h. Supply unit's blank forms or templates,

i. Any other item deemed necessary by the Appointing authority/designee.

3. Documents intended to be saved in H/Drive that begins with numbers (i.e. 1, 2, 3, etc.) as the initial identifying title should be re-named to begin with letter title (i.e., A, B, C, etc.), to avoid conflicting with the Divisional policies and procedures in H/Drive.

E. "F" Drive – Your Personal Space

1. Employees with computer authorized access and personal log-on shall save their copy of documents in their F/Drive. The documents include all documents other than those noted in Section D Item #2 above.

2. Employees may place placed in their "F Drive," the following documents:

a. Personal notes, Memos, and Memorandums,

b. Copy of Daily End of shift Reports completed at the end of the Shift.

c. Completed Incident Reports,

d. Written communication to other staff members.

e. Any other items deemed appropriate by the Appointing authority/designee.

F. G-Mail

1. G-Mail is the Division's official collaboration/e-mail software and managed by the City's ITSA. When using e-mail, employees will:

a. Consider messages to be the equivalent of letters sent on official letterhead.

b. Ensure that all e-mails are written in a professional and courteous tone.

c. E-mail messages are considered public records, copies of which may be requested by any member of the public.

2. Types of Communication

a. Unnecessary messages between users should be discouraged and limited.

b. Sender shall remove all time sensitive messages, when the message is no longer relevant. The sender does this by removing the message from sent items box and choosing remove from all mailboxes.

3. Inappropriate use of internet access or service may result in disciplinary action up to and including termination of employment, criminal action or loss of access privileges.

G. Communication Resources and Information Transmission/Interception

1. The scope of this policy is limited to those activities associated with the transmission of information using the Divisional communication resources and equipments.

2. Transmission may be intercepted and/or monitored to conduct mechanical checks, service quality control checks, maintenance of service quality, system security, and software license monitoring.

3. Transmission on the Division's communication resources may only be intercepted (including copying and/or recording) and/or monitored (including viewing and/or listening) when such interception is in the normal course of employment responsibilities, or is regarded as necessary to providing the Division's communications services, or is protecting the rights and property of the City of St. Louis. (See Mo. Ann. Stat. 542.402 (2) (3) (Supp).

4. No person may intentionally disclose information from intercepted and/or monitored transmission on the Divisional communication resources except to the person for whom it is intended, to a person reasonably involved in the process of transmitting the information to the person for whom it is intended, or to another person lawfully entitled to it.

5. The misuse or intentional disclosure of information from intercepted and/or monitored on the Division's communication network with intent to improperly obstruct or impede investigation will be a violation of this policy and will be ground for disciplinary action including and up to termination against the person(s).