# JACKSONVILLE POLICE DEPARTMENT

Policy: 4-3
Effective: 01-01-09
Revised: 01-08-21

## TECHNOLOGY MANAGEMENT

**PURPOSE**: The goal of any technology used by the Jacksonville Police Department is to maximize our effectiveness in completing our established vision. The following policy is intended to provide guidance to officers outlining appropriate and inappropriate conduct while utilizing departmental technology.

**POLICY**: It is the policy of this Department to encourage the maximum use of technology to complete our duties and responsibilities in the most efficient and effective manner. It is also the policy of this Department to discourage and eliminate all inappropriate use of technology.

**DEFINITIONS**:

I. TECHNOLOGY: Refers to computers, voicemail, electronic mail, internet access, internet/intranet e-mail, phone systems, network systems, voice and data communications, printers, copy and fax machines, video recorders, cameras, pagers, radios and any other electric equipment.

II. ARKANSAS CRIME INFORMATION CENTER: State agency responsible for providing information technology services to law enforcement and other criminal justice agencies in Arkansas.

III. TERMINAL AGENCY COORDINATOR (TAC): Someone in supervisory status that is ACIC certified or will become ACIC certified so as to better understand the requirements expected of an ACIC terminal operator. The TAC is the primary liaison between the Department and ACIC. The TAC actively represents the Police Department on matters relating to ACIC. The TAC is familiar with the record system and communication needs of the Department. The TAC keeps ACIC informed on training needs of the Department and other matters relating to the use of the ACIC/NCIC/NLETS system by the Department.

IV. DIRECTOR OF INFORMATION TECHNOLOGY (DIT): The head of the Information Technology Department for the City of Jacksonville.

V. TOKEN: A security device (wireless USB) provided by ACIC to the Department. The token generates a random password each time the officer begins the log on process for the MDT. The token acts as an electronic key.

VI. INCIDENT RESPONSE TEAM (IRT): A team of professionals that receives reports of security breaches, conducts analysis of the reports, and responds to threats to the computer systems security at the Police Department. The response team consists of: the Director of Information Technology; the Terminal Agency Coordinator; the Local Agency Security Officer; and depending on the threat, vendors could be involved.

VII. LOCAL AGENCY SECURITY OFFICER (LASO): The primary point of contact in regards to Information Security. He will actively represent the Department in all matters pertaining to information security and disseminating information security alerts.

VIII. MOBILE DATA TERMINALS (MDT): Laptop computer or other computer system utilized in the patrol vehicles.

**PROCEDURES**:

I. GENERAL

A. All users of Jacksonville Police Department technology must respect and adhere to City, State, Federal, and International laws. All use of technology must be efficient, ethical, authorized, legal, and must be consistent with the stated goal of maximizing service to our citizens.

B. No personnel should have any expectations that their use of Jacksonville Police technology is in any way private. Technology belongs to and is managed by the City of Jacksonville, and the City can and may access the technology when necessary and for any reason.

C. Supervisory personnel will generally access information contained or stored in the technology for work related non-investigatory purposes or for work related investigatory purposes related to misconduct.

II. PRIVACY

A. There should be no expectation of privacy by any employee in the use of any communication system that is operated and/or owned by the City.

B. Management has all rights to access, inspect, and monitor attachments, conversations, data, documents, emails, memory banks, messages, texts, voicemail, and any other type of employer provided electronic hardware, software, and/or storage systems.

III. COMPUTER INFORMATION NETWORK

A. Users shall promote efficient use of the computer network to minimize, and if possible, avoid congestion on the City/Department's networks and interference with the work of other users of the network.

B. No encrypting of communications is allowed without permission of the Office of the Chief of Police.

C. No "bios" or windows passwords are allowed unless approved by the Office of the Chief of Police or his designee.

D. Users shall not disrupt or damage any components of the information system.

E. Deletion, examination, copying or modification of files and/or data belonging to other users without their prior consent is prohibited.

F. Any unauthorized access or attempts to gain unauthorized access to data, system resources, passwords, etc. is prohibited.

G. Decryption of system or user passwords is prohibited.

H. The copying or deleting of network systems, operating systems and application software is prohibited unless performed by or at the direction of the City's IT personnel.

I. Any attempt to secure a higher than assigned level of privilege through the network administrator on the network or specific technologies is prohibited.

J. Software license and copyright infringement is prohibited.

K. Loading of any software in computers or networks belonging to the City is prohibited unless approved by the IT Department and/or the Office of the Chief of Police.

L. The willful introduction of computer viruses or other disruptive programs into any technology owned or operated by the City/Department is prohibited.

M. No employee shall use another employee's User ID and password, nor shall any employee attempt to secure the User ID and password of another employee. Only the employee or his Supervisors, after verification of identity, shall receive User ID and password information other