COUNTY OF MONROE
OFFICE OF THE SHERIFF
ROCHESTER, NEW YORK

GENERAL ORDER MULTI-BUREAU	DATE OF ISSUE October 3, 2025	EFFECTIVE DATE October 3, 2025	NO. 055-25
SUBJECT: GENERAL ORDER Computer Rules and Use		DISTRIBUTION All Personnel	AMENDS
REFERENCE: NYS Penal Law, Article 156.			RESCINDS 055-20

Purpose: To establish policy and procedure relative to the control and security of agency computers and computer software systems. The Information Services Unit (IS), under the supervision of the Lieutenant of Staff Services, will provide a centralized approach to software registration, accounting, and compliance with software licensing agreements. All procedures are to ensure that computer use among employees of the Monroe County Sheriff's Office (MCSO) are consistent with Monroe County policies, all applicable laws, and establish basic guidelines for appropriate and inappropriate use.

Policy: The use or dissemination of information from agency computers must conform to guidelines as set forth in this order, **MBGO-036 Central Records Unit, MBGO-053 Information Services Unit**, and Article 156 of the New York State Penal Law. It is the policy of the MCSO to ensure that all computer programs and data in the MCSO central computer system network and in individual personal computer workstations exist for the sole use of the MCSO. All employees will be responsible for any departmentally issued equipment.

I. General Guidelines and Definitions

* A. Records - any information found in the Records Management System (RMS)- Tyler (Lerms, Merge, Mobile) Inform Jail (IJ5), Traffic and Criminal Software (TraCS) , eJustice Portal, CAS, SAC, Offenderwatch, Dataworks Plus, Power DMS and other "stand alone" computer systems. Records are also defined as reports relating to investigations conducted by members of the MCSO and all data contained in criminal history folders relating to the arrest of an individual. Records further include, but are not limited to, Crime Investigation Reports, Incident Reports, Domestic Incident Reports, MVA Reports, Prisoner Data Reports, Court Commitments, Court Sealing Orders, Jail Visitor Record Cards, sealed documents, photographs, NYSIIS, and FBI criminal history reports and fingerprints.

B. Hardware - no hardware (PC's, printers, etc.) may be moved, relocated, or disposed of without written authorization from IS. No hardware may be added to any MCSO computer without written authorization from IS and installation by County Information Services.

C. Software - application software (programs) will be loaded onto Department computers by County Information Services Personnel only. All software must be approved, purchased and licensed by the MCSO IS.

1. Employees will not make unauthorized copies of software owned by the MCSO. Software that is licensed for use on one (1) computer may not be copied (or pirated) for use by another Department employee or for use by any outside third party. Employees are not permitted to bring software from home to use at work on agency

issued computers.

2. Unauthorized software (i.e., Freeware) from any outside source may not be loaded into any MCSO computer(s).

3. The MCSO is committed to standardizing software usage. Employees will use only specialized department software or other authorized installed software applications (i.e., Microsoft Word, Access, Excel, and PowerPoint, etc) to complete their work.

* D. County File Systems and Databases – any County networks, file systems, network drives, websites, and databases.

II. General Provisions for the Control and Maintenance of Computer Equipment

A. The IS maintains control over all computer equipment provided by the MCSO and has the authority to assign or relocate equipment, as necessary, in the best interests of the agency.

B. Employees are responsible for the correct operation, security, and maintenance of all MCSO computers, programs, data, hardware, peripherals, and software applications. No changes to any operating system configurations can be made without written permission from IS.

C. Budgeting approval and requisition of computer hardware and software is the responsibility of IS. Requests for computer equipment or software must be submitted, in writing, to IS. Only approved hardware and software will be installed and used in MCSO business units. This includes downloaded software and computer files obtained via the internet.

1. The IS will conduct periodic inventory audits of computer equipment to ensure compliance with this computer use policy.

2. Inspecting staff (County Information Services) will immediately remove any unauthorized hardware or software. A report documenting such will be submitted to the Commander of Staff Services.

D. Computer hardware or software will not be removed from County facilities without prior approval from the Commander of Staff Services. Users will not relocate or alter computer equipment without the approval and assistance of IS staff. As a general rule, personnel assigned laptops and/or tablets may remove those laptops or tablets from County facilities for the purpose of conducting official business only.

E. All computer-related problems (hardware issues, printers down, desktop/tablet/laptop issues, etc. network password changes, EES password changes, e-mail software issues, etc) must be reported to the County Information Services Help Desk. Technical staff will triage the problem and make referrals to the appropriate authority for follow up. Power DMS, TRACS and other MCSO Web Based software problems can be reported to Staff Services who will triage the problem and repair and change passwords for these applications. All MDC problems (hardware issues, etc.) must be reported to the Radio Center Help Desk. Users will not attempt technical repair of any agency computer equipment.

* 1. If there are widespread, prolific problems with network access, computer workstations, Dataworks Plus bookings, ejustice, Tyler RMS (Lerms, Merge & Mobile), Inform Jail (IJ5) etc. that are unscheduled and after normal business hours, the on-call County Information Services staff will be notified.

2. The shift supervisor will thoroughly investigate any problems with the previously mentioned accessibility issues before notifying on-call staff after normal business hours.

III. Security and Backup of Agency Computers and Peripherals

A. Security access to computer networks and systems will be assigned by the Commander of Staff Services or designee who will make the request to MCSO IS or County Information Services Unit on an individual basis.

B. User ID's and passwords will be provided to staff for network access and server based applications. All network accounts will need to be logged into the network within 30 days to reset the generic password. All employees can change their own network passwords by hitting the Ctrl-Alt-Delete buttons on their keyboards. All employees will enroll in the AD Self Service Plus Client Software popup window after they log in the first time. Requests for system access must be submitted by filling out a MB-150 User Account Creation Form for review and processing to IS.

C. Passwords must be kept confidential. Sharing, using, or attempting to use the password of another person is prohibited, unless authorized by the Commander of Staff Services.

D. When a password is believed to have been compromised, the County IS Help Desk will be notified immediately so that the password can be changed.

E. Users signed on the system are responsible for all changes made with their sign-on. For security purposes, all computers will automatically go into a sleep state after two (2) minutes of inactivity.

Note: All computer accesses, or attempts to access, are captured by the respective computer system and are reviewed by the County IS Network Team. Changes to critical files are also captured by the computer, as well as the date, time, device, password, and before/after images of data records. Unauthorized changes to computer data are a violation of this Order and may be a violation of the New York State Penal Law.

F. All employees who are issued memory sticks or have external hardware devices and attach them to a County computer will have Bitlocker apply encryption to files placed on these drives.

IV. Security Process

A. MCSO will have a security process in place including, but not limited to all employees, vendors, DES, County IS employees, and contractors who have physical and/or logical access to applications, systems, infrastructure or data governed by interagency agreement(s) between Information technology Services and any public safety agency.

B. Prior to obtaining access to Public Safety applications, systems, infrastructure or data, all employees, vendors, DES, County Information System employees, contractors and others not defined, shall be directed to be fingerprinted by Sheriff's Central Records Staff.

* C. All County Employees (DES, County IS, Interns, etc.) will be required to complete the CJIS Security Policy Awareness Training. Once completed, the user will fill out the CJIS Security Policy Form and send it to MCSO IS for tracking. All personnel will need to comply with this training every year. MCSO IS will track all training and will send a list to each department for completion.

D. Sheriff's Central Records shall conduct a state "Search and Retain" criminal history records check and federal criminal justice site security check. The search results will be forwarded to the Commander of Staff Services.

* E. The search results will be forwarded to the MCSO IS/ eJustice TAC (Terminal Agency Coordinator).

* F. The Commander of Staff Services (eJustice LASO) shall make a determination regarding the applicant's suitability for an assignment involving potential physical and/or logical access to Public Safety applications, systems, infrastructure or data on a case by case basis, where timely assignment is needed. If the Commander denies access, MCSO IS (TAC) will send an email to the County Department Head advising of the status.

G. If the assignee is subsequently arrested, the Commander of Staff Services will receive a hit notice advising of the arrest and the assignee access will be immediately revoked.

* H. All MCSO employees who have access to the eJustice NY Integrated Justice Portal, will successfully complete the Portal Certification Test to gain access. Recertification will occur every year. The Sheriff's Central Records sub-TAC will complete all accounts with the exception of the Jail Bureau. The TAC & CJIS will send you recertification emails to complete the test. The Jail Tac will complete the jail account and send recertification emails.

V. User Account Access

A. New Recruits

1. New Recruit Deputies will get the following user account access when they start the academy:

   a. Outlook (Email) account
   b. PowerDMS account
   * c. eJustice Account
   * d. Dataworks Plus accounts (Police and Civil Bureau)
   * e. Tyler (Mobile) account (Police and Civil Bureau)

2. Once Recruit Deputies are assigned on probationary assignment, they will get the following user account access:

   a. Network User account
   b. CAD User account
   c. IJ5 (Jail Bureau)
   d. TraCS (Police Bureau)
   e. Internet Access

B. New Civilian employees - New civilian employees, to include but not limited to, Institutional Helpers and Trainees, will get the following user accounts when they start employment:

1. Network User account
2. PowerDMS account
3. Outlook (Email) account
4. Internet Access
5. If additional software applications are needed due to assignment, please fill out an User Account Creation Form (MB-150) and forward to Staff Services for final approval.

* C. Employees of MCSO are subject to County IS policies and required to complete the County's mandatory online training (KnowBe4). The County IS policies that each employee agrees to comply with are listed on the Intranet under County Policies and currently include:

1. Artificial Intelligence Policy

2. Data Sharing Policy
3. Technology Use Policy
4. Breach Notification Policy
5. Social Media Policy

D. Promoted Sworn employees - When sworn employees are promoted from one rank to another, he/she will get the following accounts updated after completion of their STO.

1. Network Account updated

2. Subpoenas Database (Police Bureau) granted

E. Transferred employees - When a Personnel Order has been ordered for employees who are being transferred from one assignment to another, their network account will be transferred the following Monday due to resources at County Information Services.

Note: Any need to have your account moved/transferred sooner than the date on the Personnel Order, please send an email to the Commander of Staff Services for approval.

* F. On an annual basis Staff Services will complete an audit of folder and group membership in order to maintain file security and prevent any unauthorized access.

* G. Unauthorized Access – If an employee becomes aware that they have knowingly or mistakenly been given access to Records, Software, County File Systems, and Databases that are not pertinent to their role or job assignment, such employee has a duty to notify the Commander of Staff Services as soon as the employee learns of such access. The employee shall not access or review such Records, Software, County File Systems and Databases nor attempt to ascertain any information contained in such Records, Software, County File, and Databases unless specifically authorized by the Commander of Staff Services.

Note: The duty to report unauthorized access to Records, Software, County File Systems, and Databases is part of the broader responsibility to protect the organization's information and ensure compliance with relevant laws and regulations, including but not limited to other employees' private and medical information.

VI. Employer Rights

A. The Sheriff reserves (and intends to exercise) the rights to access, monitor, update, or delete certain programs or functions in order to protect the integrity of the MCSO Computer Network. Additionally the Sheriff may disclose contents of e-mail messages for the following reasons:

1. Compliance with an investigation into suspected criminal acts, investigations of suspected breeches of security, or violations of MCSO policies.

2. Recovering from system failures, finding lost information, or other emergencies.

3. Evaluating the effectiveness of electronic mail and to provide assistance when employees are out of the office, or are otherwise unavailable.

4. Any other reason deemed appropriate by the Sheriff or their designee.

B. The Sheriff will reserve the right to log network computer use, monitor file server space being used, and remove user accounts from the network.

VII. Use of Departmental E-Mail

Employees will not send large files or send inappropriate messages to large numbers of recipients that may unnecessarily consume network resources that are required for other MCSO business. When the Sheriff grants an employee internet access or an e-mail account, it is the responsibility of the employee to adhere to the following guidelines:

A. Messages must not include remarks or content that is threatening, insulting, obscene, abusive, derogatory, or constitute harassment of any type.

B. Messages will not be used for illegal or unethical activities, be political, or religious in nature.

C. Messages will not involve personal sales or solicitation or be associated with any profit or not-for-profit outside business activity.

D. Files are to be housecleaned at least once a month, deleting any old e-mail or downloaded information. Information can be stored on appropriate media if necessary.

E. All employees are required to open and review their department e-mail accounts at least once during their tour-of-duty.

F. All employees can have an archive setup for them by the County IS Help Desk if they need to save emails for future archival.

VIII. Use of the Internet

The connection to the internet exists to facilitate the official work of the MCSO. Use of the internet will be for business related use only. Internet access is monitored for amount of usage along with the names of the web sites that are accessed. All users of the internet will adhere to the following guidelines:

A. The internet will not be used for personal recreation, playing games, any type of illegal activity, participation in chat rooms/groups, or for the propagation of computer viruses.

B. The internet will not be accessed to transmit, receive, copy, or download any material or correspondence that could be considered threatening, obscene, or harassing in any form.

C. Staff will not use any internet service for private marketing, business transactions, unauthorized distribution, disclosure/use of departmental data and information, or for private advertising of products and services.

D. Internet usage will not involve personal sales, solicitation of political or religious causes, or be associated with any profit or not-for-profit outside business activity.

E. Internet usage, however, will not be restricted for the purposes of conducting legitimate criminal investigations or research pertaining to the Sheriff's Office.

Note: Any internet site used on department owned/maintained computers may be subject to release to the public under the Freedom of Information Act.

F. An internal review of employees who have been granted use of the internet will be conducted by the County IS Unit and by the Commander of Staff Services who will then report their findings to the Undersheriff every six (6) months.

IX. Server Backup Procedures

County Information Services-will be responsible for the establishment and revision of file backup procedures for all services under the control of the MCSO. These written procedures will be maintained by the Information Services Unit and will be reviewed by the Commander of Staff Services on a semi-annual basis. Files saved on individual hard drives, disks, CD, etc are the responsibility of the employee and are not the responsibility of the IS Unit.

X. Mobile Data Computers (MDC's)

MDC's will be governed by the same general provisions as previously mentioned in Section V and Section VI of this Order, as well as the provisions outlined in **PBGO-046 Communications**.

A. Messages or transmissions must not include remarks or content that is threatening, insulting, obscene, abusive, derogatory, or constitute harassment of any type.

B. Messages or transmissions will not be used for illegal or unethical activities, be political, or be religious in nature.

C. Messages or transmissions will not involve personal sales or solicitation, or be associated with any profit or not-for-profit outside business activity.

D. Transmissions and/or reports will be business related only.

XI. Disposal Process of Information

A. All information will be securely disposed of according to its sensitivity in an approved manner that renders the information useless unless otherwise governed by legislative or regulatory requirements. Such items requiring disposal can include but are not limited to:

1. Fixed hard disks in PC's and copiers.
2. Memory sticks (which should be reformatted to allow for data deletion).
3. All used CD's or DVD's (which should be destroyed by either shredding them or by destroying their data.
4. Any equipment that could contain storage media.

B. These items must be checked to ensure that any information or licensed software is removed or overwritten prior to disposal.

By Order of the Sheriff,

Todd K. Baxter

* Indicates significant changes from the previous Order.