1.01-7 DAYTON POLICE DEPARTMENT

GENERAL ORDER

MANAGEMENT INFORMATION SYSTEM (MIS), KRONOS TIMEKEEPING AND DATA SECURITY

RICHARD S. BIEHL – DIRECTOR AND CHIEF OF POLICE

Rev. 05/20

POLICY STATEMENT

It is the policy of the Dayton Police Department that information contained within the MIS, OHLEG, Accurint, JusticeWeb, and KRONOS Timekeeping System and all their adjoining modules is potentially sensitive and that the information will be maintained in the strictest confidentiality to conform to the guidelines of LEADS and NCIC. All usage of these systems will be treated as confidential and for official use only. Dayton Police personnel are never permitted to access these information sources for personal use. Abuse or improper usage of these confidential systems demonstrates an extreme breach of propriety and will result in disciplinary action.

Further, the use of FAT Clients (PC's and Laptops), as well as THIN Clients will be done is such a manner as to ensure the security of the devices and the systems accessible by those devices. All personnel using the system(s) will be accountable for any abuse while under their unique Login and Password.

I. MANAGEMENT INFORMATION SYSTEM (MIS)

A. The Dayton Police Department operates a Management Information System (MIS). MIS has the capability of compiling statistical and/or data summaries of the following department activities:

1. Police Personnel
2. Wanted Persons/Warrants
3. Calls for Service
4. Incident Reports
5. Field Contacts (Warnings, FIC's, Removals, etc.)
6. Towed Vehicle Control
7. Pawnshops
8. Master Index (Wildcard search of names, SSN, etc.)
9. Property and Evidence
10. Alarms
11. Stolen Vehicles
12. Arrest/booking
13. Citations (Moving, Parking and Minor Misdemeanor)
14. Permits

Requests for MIS information and crime stats will be directed to the Statistical Analyst, CAD (Computer Aided Dispatch) information can be requested through the Regional Dispatch Center (RDC) staff.

B. The information contained within CAD and MIS is generally accepted as confidential, police-only information that cannot be given to unauthorized non-sworn personnel if it contains sensitive information, or LEADS, NCIC information. Officers/personnel must use caution to ensure that unauthorized non-sworn personnel do not gain access to Social Security Numbers (SSN), dates of birth (DOB), addresses, phone numbers, license numbers, or any information that by its very nature appears to be sensitive. Additionally, no information concerning an investigation in-progress should be shared without proper management review.

C. Officers requesting the deletion of arrest records in MIS (e.g. erroneous arrest record, person not actually incarcerated after sending the record, etc.) will be required to send an E-mail with the information and reason for deletion to the Strategic Planning Bureau Commander for review and a "cc" to their immediate supervisor. The Bureau Commander will review the request and forward to the MIS Administrator for deletion.

II. KRONOS TIMEKEEPING SYSTEM

Personnel Action Entries

A. **LEAVE REQUESTS** - Employees requesting vacation, personal allowance, compensatory or holiday leave must submit their leave requests to the supervisor that will approve the request and enter the change into KRONOS via the electronic leave request process.

- Each individual's supervisor will be responsible for approving/denying the leave request prior to the occurrence of the event. Leave balances must be verified before any leave is approved.

B. **DAY DUE** - Employees may only be placed on a day due if they worked due to a change in work schedule or were re-scheduled for training purposes.

1. All days due must be entered into KRONOS prior to the employee using the day due.

2. Only the next level supervisor will approve an employee's day due leave request.

3. When a day due is taken, the request approval in KRONOS must indicate in the comments section the day that was worked to earn the day due.

4. A day due must be taken within the FLSA 28 day cycle of the original day that was worked to earn the day due.

C. **SPECIAL ASSIGNMENTS** - Anytime an employee is placed on Special Assignment, the remarks section in KRONOS must contain a complete description of the special assignment, including hours of work, reason for the special assignment and location where the special assignment will be.

1. The starting and ending time fields of the assignment must match the stated times in the remarks section.

2. If the employee is temporarily changing work assignments (ASN's), that employee will be scheduled to work the hours of the unit to which they are being assigned. Any deviation must be approved by the Division Commander, and Police Payroll must be notified in advance. The employee's immediate supervisor will ensure that the information is correctly entered into KRONOS.

3. Changes to KRONOS work schedules that are beyond the supervisor's security level will be made by a request via e-mail to police payroll personnel. No other personnel will be authorized to make these changes.

D. **Trade Days for Sworn Personnel** - sworn personnel will only be permitted to trade days with other personnel who have the day off on the day they wish to trade (i.e. an officer wants a Friday off and the person they are trading with is on regular days off that Friday) and that are within the same twenty-eight (28) day Fair Labor Standards Act cycle. Sworn personnel will only be permitted five (5) trade days per calendar year.

E. It is the responsibility of each supervisor to ensure that their employee's time entries into the KRONOS Timekeeping System are accurate This applies to all regular shifts, overtime assignments, special details, etc. The supervisor will ensure that KRONOS Timekeeping System entries are amended if there are any changes that affect the accuracy of the employee's time record. Changes to KRONOS Timekeeping System entries must be entered as soon as a supervisor learns of them.

F. **VLS** - When a supervisor presents findings of charges and specifications to an employee and suspension days are mandated, the employee will choose to take either suspension or vacation in lieu of suspension (VLS) if applicable.

If the employee chooses VLS, the supervisor must document it appropriately on the suspension form. The supervisor will enter into KRONOS an "**add"** for a VLS pay code on the effective dates. VLS must be served on actual days of work. Do **not** remove the normal shift hours the employee is scheduled to work. The supervisor will print the schedule and attach it to the suspension form, showing that the entries have been made.

Payroll personnel will verify that the entries are made appropriately upon receipt.

G. **CRT** - the Court Detail will enter all court appearances for sworn personnel into KRONOS. The Court Appearance code will be "CRT" and the entry may be viewed on Schedule Editor. With the exception of an employee's annual guaranteed vacation all supervisors will check for any court appearances scheduled PRIOR to granting leave requests. If there is a scheduled court case/proceeding, the employee will be reminded of their obligation to attend. Supervisors will also remind the employee that they are NOT ELIGIBLE for the contractual day-off premium for their attendance which is paid only on a regularly scheduled day off or annual guaranteed vacation.

This General Order supersedes all prior rules, regulations, policies and procedures, whether oral, written or by previous practice.

H. **VGA** - supervisors will enter their personnel's annual guaranteed vacation into the KRONOS Scheduler by March 15th of each year. The pay code to enter the annual guaranteed vacation leave into the schedule will be "**VGA.**" The VGA pay code should be used whenever an Officer officially requests and is approved for his/her guaranteed vacation.

The VGA pay code works the same as the VAC pay code and it also serves as a "place marker" to assist with Court scheduling.

If the employee does not use all of their guaranteed vacation leave on the dates requested or the dates are subsequently changed by mutual agreement of both the employee and Management, the VGA pay code can be moved and added or deleted as required.

I. **General KRONOS Rules:**

1. **ALL** KRONOS actions must be entered and approved by an employee's supervisor. Supervisors cannot approve your own Overtime or Compensatory Time Accrual.
2. Supervisors are not permitted to enter and approve their own Leave, or Schedule changes.
3. Clocking in or out for another employee is strictly prohibited and will result in immediate discharge.
4. All hourly personnel will be issued a separate identification card to be used with the KRONOS system.
5. Employees must maintain their card in good working order, surrender the card when requested by a Supervisor, and immediately notify Supervision if the card is not working correctly or is lost.
6. Cards needing to be replaced within two (2) years of issue will require a $5.00 replacement fee unless the employee can show the card was damaged during the course of employment.
7. Employees must use their ID card to punch, not the KRONOS time clock key pad.
8. All non-exempt (hourly) employees are required to use a KRONOS clock to punch in at the start and end of the shift, for non-paid meal periods, and whenever approved leave is taken mid-shift for non-City business (e.g., a doctor's appointment, personal leave, etc.). If a KRONOS clock is not near a work reporting location or other operational factors make the use of the clock impractical as determined by Management, an alternate method of time reporting, approved by Human Resources, must be used (i.e. via a computer terminal or "Green Time Sheets").
9. Unless it is in conjunction with scheduled or approved OT, non-exempt (hourly) employees are not permitted to punch in more than six (6) minutes before the scheduled start of the shift and not more than six (6) minutes after the scheduled end of the shift. This is for a regular work day when an employee is not required to work overtime hours connected to the beginning or end of the scheduled work day.
10. Eligible exempt employees must use the KRONOS clock for any authorized OT hours. The KRONOS clock is not used to record regular scheduled hours for exempt employees. If a KRONOS clock is not near a work reporting location, an alternate method of overtime reporting must be used, i.e. "Green Time Sheets."
11. Employees can also use the clock to:
    - Check leave balances
    - Check their work schedule
    - Check punch status

J. **KRONOS Clock Restrictions:**

1. Employees are not permitted to punch in seven (7) or more minutes before the start of the shift (unless it is in conjunction with approved OT) and most KRONOS clocks will not accept a punch during this time period.

   For example, an employee's work shift begins at 7:00 a.m. and they arrive a little early at their work reporting location at 6:45 a.m. The earliest that the employee could punch in is 6:54 a.m. and they must not start working until the start of their shift, which is 7:00 a.m.

2. Clocking out before the end of the shift is not permitted unless it is done in conjunction with approved leave.

3. In general, hourly employees are not permitted to be at their work location unless it is immediately prior to the start or end of their work shift.

4. Hourly employees are not permitted to begin work before clocking in or to continue working after clocking out.

K. **Rounding of clock-in and clock-out punches**

1. In accordance with the FLSA regulations, "rounding" of hours worked is permitted as long as the rounding is done in such a manner as to "average" out time to ensure that employees are fully compensated for all time actually worked. Thus "rounding" works both ways – "for" and "against" the employer and the employee.

2. In KRONOS, hours are counted in .1 hour (6 minute) intervals.

3. Early clock-in is not permitted unless in conjunction with call-in or approved OT.

4. The above rounding rules apply only to scheduled hours. There is no rounding of time for unscheduled hours.

L. **Leave Accrual/Usage**

1. Sick leave and vacation are added to a full-time employee's leave balance after he/she has worked (regular hours excluding overtime) and/or has been on paid leave for 80 hours in a calendar month. Leave is available for use on the work day following the day on which the 80th hour is worked.

2. Personal leave is credited on January 1st of each year. Personal leave is available for use on January 2.

3. Vacation, sick and personal leave credits are deducted from employee leave balances when the leave is used. Pre-approved leave is also deducted on the date it is used, not on the date it is approved.

4. Leave is granted in one (1) hour increments and must also be used in one (1) hour increments.

5. Official leave balances will be kept in KRONOS, not on paper documents.

6. Both exempt and non-exempt employees can access their leave balances at the time clock.

7. MAXIMUM allowable accumulations of various forms of Accrual:

   - Comp Time – **176 hours**
   - Vacation Time (Sworn) – **492 hours** (240 hours carry-over from previous year + 96 hours (8 hrs per month) + 96 hours for Seniority Supplemental Accrual + 60 hours Conversion of Sick Leave = 492 maximum hours
   - Vacation Time (Non-Sworn) – **476 hours**
   - Sick Leave – both Sworn and Non-Sworn can earn up to **1140 hours**, but can only carry-over 1120 hours. (The maximum is set at 1140 hours in KRONOS; 1120 hours + 20 extra hours – two months

accrual – to ensure employees have the opportunity at the beginning of the year to convert Sick Leave to Vacation/PA.)

If an employee goes over their maximum allowable balance, KRONOS will automatically default back to the maximum allowable balance each day and the employee may lose their additional time. It is imperative that officers and their supervisors not enter or approve comp time accruals in excess of the **176** hour limit. At the end of the day, the balance will reconcile to the allowable maximum of 176 hours and the employee may lose the extra time.

M. **Overtime**

1. All authorized overtime must be approved by a Supervisor using the employee's time card in KRONOS. If the OT is the result of working through a non-paid meal period, the Supervisor must cancel the automatic meal time deduction in KRONOS. To the extent practicable, employees are not permitted to work through their non-paid meal period without prior approval of Supervision.

2. Regular time and/or overtime worked that is not authorized by Management will be subject to disciplinary action.

3. When supervisors enter an officer's overtime assignment into KRONOS, they are required to add comments to the entry and indicate the hours that the officer worked the overtime assignment.

4. The following procedure will be used when requesting pay/comp for overtime:

- Officer sends an email to a supervisor requesting overtime pay/compensatory time.
- Supervisor makes and/or approves the time entry in KRONOS.
- Supervisor types a reply to the original officer email, saying, "Approved. Please double check entry for accuracy."
- Supervisor cc's that reply to "DPD – Payroll Clerks".
- Supervisor sends the email (to the original officer and to the Payroll Clerks).
- Supervisor is no longer required to keep the email from the officer.

Payroll clerks, already with an alphabet system in place, move the email to the officer's overtime folder for the year on their H: drives. This group is responsible for electronically archiving the emails per retention schedules.

N. **Non-paid Meal Breaks**

1. Non-exempt employees are required to clock out and in for non-paid meal periods unless Management determines that using the KRONOS clock is impractical due to operational factors. Non-exempt employees who do not clock for non-paid meal periods are required to maintain their actual time spent not working during their non-paid meal period using a "Green Time Sheet."

2. Generally, full-time employees are assigned one (1) of three (3) scheduled non-paid meal periods:

- Straight eight (8) hour work schedule with no non-paid meal period
- 8.5 hour work schedule with a non-paid 30-minute meal period
- 9 hour work schedule with a non-paid 60-minute meal period

3. Employees are required to clock back in from their non-paid meal period within their designated 30- or 60-minute non-paid meal period.

4. Clocking in or returning early (more than five (5) minutes) from an employee's scheduled non-paid meal period without Supervisory approval creates unauthorized overtime (UN-OT) and will be grounds for disciplinary action.

5. Clocking in or returning one (1) to 30 (thirty) or more minutes late from an employee's scheduled non-paid meal period is considered tardy and counts as an occurrence under the Tardiness/AWOL Guidelines.

6. Clocking in or returning more than 30 (thirty) minutes late from an employee's scheduled non-paid meal period will be considered AWOL.

7. Non-paid meal periods must be taken at their regularly scheduled time and for the allotted time period unless otherwise authorized by a Supervisor to change the scheduled time or duration.

8. S-96 Employee Weekly Time Records

   Officers and sergeants who do not normally go on duty via radio and MCT (i.e. Operations Divisions) are required to document their meal breaks by completing an S-96 Employee Weekly Time Record "Green Sheet" to document this information.

   The time records are to be completed on a weekly basis and submitted to the employee's immediate supervisor, who will store them, on-site for a period of 2 years. (See General Order 1.01-1)

O. Tardiness/AWOL Guidelines

1. Tardiness is defined as clocking in late from one (1) to 30 (thirty) minutes after an employee's scheduled start time or clocking in or returning one (1) to 30 (thirty) minutes late from an employee's scheduled non-paid meal period.

2. Listed below are the corrective actions that apply when an employee has a tardy occurrence within the past 12-month rotating period, and the occurrence is 30 (thirty) minutes or less:

<u>Occurrence</u>	<u>Corrective Action</u>
1	Non-Disciplinary Employee Counseling No. 1
2	Non-Disciplinary Employee Counseling No. 2
3	Training Memorandum
4 or more	Progressive Discipline starts with an Oral Reprimand

III. <u>DESKTOP DEVICES FOR INFORMATION ACCESS</u>

The police department has acquired FAT Clients (PC's and Laptop Computers), as well as THIN Clients (TC's) for the purpose of automating many management, clerical functions, and police operations. PC's, Laptop Computers, and TC's are all examples of "desktop devices," and security measures will apply to them interchangeably, where applicable. Desktop devices require departmental and/or City standards for a number of related issues: acceptable software, loading foreign files/diskettes, downloading and taking information home, copyright protected software, confidentiality of information, sharing information, point of access security, and related issues.

A. The following police department <u>software</u> purchasing, licensing, and installation standards are in effect:

1. Acceptable or authorized program software is defined as software that has been approved for department use by the Chief of Police and/or is supported through the City of Dayton Information and Technology Services Department (IT). In order for software to be approved by the Chief of Police, all software purchases <u>must</u> be coordinated and approved through the police department fiscal manager after being reviewed by the assigned IT Analyst.

2. The Department of Information and Technology Services will install all application and operating system software to verify licensing compliance and suitability for use on the City's Enterprise System(s).

3. Any inappropriate use, loading, downloading or copying of information and/or program software from or onto any Police Department or City owned and/or controlled computer or PC is strictly prohibited. This includes games of any kind.

4. Illegal duplication or use of illegally duplicated software is a crime. Copyright protection of software must be maintained. Unless specifically exempted by documented licensing agreements, a software program must reside on only a single PC at any time. Also, each user site, unless exempted by licensing agreement, must possess a registered copy of the software program being used together with the

accompanying documentation and original license. Violations of this section could subject the City to Criminal and/or Civil action. Abuse will not be tolerated.

a. No City-owned software should be installed on any non City-owned desktop device without prior written consent of the Department of IT.

b. No non City-owned software should be installed on any City-owned desktop device.

5. No employee will install or allow the installation of any application or operating system software onto any City-owned PC without the knowledge and consent of the Department of Information and Technology Services. (No personally owned, non-City software or hardware is allowed on the City's systems or networks without the prior written consent of the Department of IT).

6. No employee will uninstall or purposely defeat or compromise any virus scanning software placed on any City equipment. All PC's used by the City that are connected to the Enterprise network will have and maintain the updated virus scanning software package as specified by the Department of IT.

7. Antivirus (malware) Software Policies & Procedures

The City of Dayton IT division provides malware protection for computers via Microsoft Forefront's enterprise antivirus product. This document covers policies and procedures for malware protection of computer systems overall in the City and specifically for the Police Department personnel.

The Forefront software tool protects City systems from viruses, worms, Trojans, computer "bombs", and other forms of intentionally destructive software, as well as annoying but generally non-destructive software pranks. These types of malware, if not controlled, can create situations of information loss, lost productivity, to extensive and expensive system outages.

Adherence to the policies and procedures herein will reduce instances of getting "infected" by malware on City computers. LEADS also requires DPD personnel be trained and aware of malware/antivirus policies and procedures.

a. Forefront Antivirus Deployment

- Forefront antivirus product is deployed on all City workstations, laptops, and servers by the IT organization. Coverage for thin client workstation operation is handled at the Citrix server farm level. Support for it is through the Help Desk.

- Malware / Antivirus software should be implemented for employee personal equipment (for home use) regardless of whether or not such personal equipment is brought into the office or used for work.

- Individuals are responsible to install the appropriate malware / antivirus software on their personal equipment and keep it updated. Support for this software shall be with the vendor you purchased the software from. It does not necessarily have to be a Microsoft Forefront product.

b. Policies

All general-purpose computers deployed by and used for City of Dayton purposes must operate an up to date version of the Forefront client software with the most currently available signature file. This is a requirement when a computer is:

- Unconnected/free-standing where files may subsequently be transferred to other City machines via some media (diskettes, CD's, DVD's, thumb drives)
- Connected with City of Dayton networks
- A personal computer brought into the office
- A city issued or personal computer used to remote into the City network

Computers should be allowed to operate on the City's network long enough in order to properly receive updated signature files and to perform virus-scanning operations. File updates are automatically handled by the computer when connected to the City network and generally scheduled between 12:30 PM and 1:00 PM.

It is a requirement on personal equipment to have an up to date malware / antivirus program running if it is used to remote into the City of Dayton networks or if media (diskettes, CD's, DVD's, Thumb Drives, etc.) is used on them where files are intended to be transferred to City equipment. Such media shall be scanned for viruses prior to transfer to other City computers or file servers.

Users shall not disable the Forefront antivirus services on City provided equipment.

c. Support for Microsoft Forefront

The IT Help Desk at 937-333-2748 provides support for Forefront antivirus services. City workstations, laptops, and thin clients are pre-configured with Forefront antivirus. Non-administrative users are restricted to the settings provided by IT. There are no user-configurable settings.

Contact the IT Help Desk in troubleshooting situations where Forefront is suspected in operating system or application problems.

d. Procedures for Forefront Anti-Virus

1. For full PC workstations and laptops make sure the Forefront service is running. You will see the following icon in the systray in the lower right hand corner of your screen:

   🛡

   Contact the IT Help Desk at 937-333-2748 if this icon is not running on the computer. **Note:** this icon will not appear on thin clients. Forefront antivirus runs on the Citrix servers behind the scenes on thin clients.

2. Do not open attachments in E-Mail if you have any doubt about, or are distrustful of, who sent you the attachment. Delete the E-Mail without opening the attachment.

3. Manually scan media (CD's, DVD's, diskettes, thumb drives, etc.) using Forefront when you intend to transfer the contents to your computer or network drive. The following is the procedure to do this:

   http://technet.microsoft.com/en-us/library/ff823797.aspx

   Look under the section titled "Running a custom scan".

4. Do not surf nefarious or potentially risky Web sites; particularly file sharing or music download sites. These are notorious for infecting computers. Even though the City's Barracuda system controls Web surfing by content type categories, risky sites can still be potentially accessed. Stick to business and professional sites that can be trusted.

5. Using Web-based personal E-Mail sites (Yahoo, AOL, MSN, Hotmail) are entry points for chain letters, Trojans, or viruses. Avoid using the City network and Internet connection for personal E-Mails.

6. Laptop users who access the web from DSL and Cable modems from home or wireless networks in coffee shops and hotel lobbies are at high risk for data theft, or having malware implanted onto their open shares. Password stealers, backdoor programs, and Denial of Service agents can all be surreptitiously installed on an exposed laptop, which then becomes a type of Trojan horse when it logs onto a network that trusts it. Contact the IT Help Desk to educate yourself to the dangers of logging into wireless networks at home, in hotel and airport lobbies, coffee shops, and other public networks.

7. If you feel you may have your full PC or laptop infected with malware take a moment to manually scan your local disk drives. Contact the Help Desk and advise them of the situation.

B. Access to the Ohio Law Enforcement Gateway Database (OHLEG) and the Accurint (Lexis-Nexis) Database is available through Internet Access on the City of Dayton Citrix Network with the following restrictions:

1. This information is strictly for Law Enforcement use only.

2. Internal programs will log each employee's use of each Database.

3. This information is not to be disseminated to the public and is to be treated the same as LEADS information following the same security protocols.

Microsoft Windows Operating Systems are the standard operating system for all City of Dayton owned personal computers.

C. The following police department hardware purchasing, and installation standards are in effect:

1. Acceptable or authorized hardware (PC's, Laptops, CD Drives, DVD Drives, Zip Drives, Printers, Scanners, PDA's, etc.) is defined as hardware that has been approved for department use by the Chief of Police and/or is supported through the City of Dayton Information and Technology Services Department (IT). In order for hardware to be approved by the Chief of Police, all hardware purchases must be coordinated and approved through the police department fiscal manager after being reviewed by the assigned IT Analyst.

2. All equipment must be checked in by IT to ensure that it is audited, placed into the City's database(s), and receives a City 'asset control tag.' No procurement of hardware shall take place without an assessment by an IT Analyst, including P-Card purchases.

3. No personally owned, non-City equipment is allowed on the City's networks without the prior written consent of the Department of IT.

4. None of the above applies to normal consumables like paper, cartridges, ribbons, batteries, etc.

D. The following Security and Proper Use Procedures will be in effect:

1. No employee will share their Login or Password with any other employee. Any violation of use or misuse/abuse will be Prima Facie evidence of abuse by the employee whose Login and Password was used at the time of the infraction. Caution must be used when walking away from an unsecured desktop to ensure that the keyboard is locked or the user has 'logged off' the system.

   a. If any employee has reason to believe their password has been compromised, they are advised to set a new password. In this MIS, this can be done from the opening screen.

   b. If an employee fails to log on correctly after a number of times, the system will automatically lock their account for security purposes. Should that happen, the user must contact the MIS Manager, not the IT Help-Desk, to have their account unlocked.

2. No employee will knowingly use the Login and Password of another.

3. No unauthorized Internet accounts (i.e. DSL, Cable, etc.) will be allowed. Permission for any such account must be requested in the form of a special report to the Chief of Police and must describe the purpose for the account, the mechanism for supporting this account (funding), the security measures that the employee will maintain to ensure that the City is not compromised. Once approved, the Department of IT will ensure the installation is in accordance with the security standards in place at that time by IT.

4. Abuse of the Internet and/or the City's Email system will not be tolerated. Employees are encouraged to use appropriate etiquette and to refer to the City's Personal Policies and Procedures Manual, Section 2.14.

E. The following Compliance Auditing procedures will be in effect:

1. To ensure compliance with this order, all Desktop Devices in the police department will be randomly audited. The Department of IT will remove all software that is found not to be in compliance the above policy. Names of violators will be turned over to the Chief of Police. All violations will be investigated. Any violation that would put the City into a position of copyright or licensure liability with a software vendor will result in disciplinary action.

2. The Department of IT will also record the serial numbers, makes, models, etc., of all hardware that is found not to be in compliance the above policy. This is to ensure that the information is contained in the City's database(s) and that the device receives an 'asset tag.' Names of violators will be turned over to the Chief of Police. All violations will be investigated.

3. Anyone having questions about licensing agreements and software support should contact the IT Help Desk at 333-4357.

IV. LEADS INFORMATION SECURITY

The Dayton Police Department makes extensive use of information obtained from LEADS (Law Enforcement Automated Data System) and NCIC (National Crime Information Center). Similarly, we create numerous records in these systems which assist in the detection and capture of criminal suspects, missing persons, stolen property, and provide information that promotes officer safety. (This information is herein referred to as CJIS ((Criminal Justice Information Services)) information.)

A. The TAC (Terminal Agency Coordinator) will coordinate the training and certification of personnel who will have access to CJIS information.

B. Training and certification is required prior to the granting of a computer account that will access CJIS information and for continued use of those accounts.

C. State and national fingerprint-based record checks must be conducted within thirty (30) days of initial employment or assignment of all personnel who have authorized access to LEADS/CJIS systems, record storage areas containing LEADS/CJIS data and those who have direct responsibility to configure and maintain computer systems and networks with direct access to LEADS/CJIS systems.

D. Certification must occur every two years. Personnel who do not maintain certification will be denied access to CJIS information to include the deactivation or downgrading of applicable computer accounts.

E. The LEADS Administrative Rules are incorporated herein and must be adhered to. (LEADS training specifically delineates the requirements of the LEADS Administrative Rules.)

F. The LEADS newsletter contains updates from LEADS and NCIC and constitutes an official communication. Personnel are required to read the LEADS newsletter. The TAC is responsible for disseminating the newsletter.

G. Employees who violate the requirements of the LEADS Administrative Rules are subject to disciplinary action in accordance with pertinent labor contracts and administrative rules of the City of Dayton and Police Department. Where applicable, violations of the LEADS Administrative Rules may result in criminal prosecution under state law and/or federal code for unauthorized use of property, theft, tampering, receiving stolen property, and unauthorized access to computer systems or any other applicable federal or state law. Among other LEADS restrictions, employees are prohibited from:

- Using LEADS for non-criminal justice purposes,
- Giving LEADS information to unauthorized people,
- Using someone else's login,
- Leaving a computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access Dayton Police Department systems and or FBI CJI systems in your name,

- Allowing unauthorized persons access to FBI CJI systems at any time for any reason. (Unauthorized use of FBI CJI systems is prohibited and may be subject to criminal and/or civil penalties),

- Allowing remote access of Dayton Police Department issued computer equipment to FBI CJI systems and/or data without prior authorization by the Chief of Police or their designee,

- Obtaining a computer account that you are unauthorized to use,

- Obtaining a password for a computer account for another account owner,

- Using the Dayton Police Department network to gain unauthorized access to FBI CJI,

- Knowingly perform an at which will interfere with the normal operation of FBI CJIS systems,

- Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security gaps to FBI CJI systems,

- Violating terms of software and/or operating system licensing agreements or copyright laws,

- Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in the Dayton Police Department, for home use or for any customer or contractor,

- Masking the identity of an account or machine,

- Maintaining FBI CJI or duplicate copies of official Dayton Police Department files in either manual or electronic formats at place of residence or in other physically non-secure locations with express permission,

- Using Dayton Police Department's technology resources and of FBI CJI systems for personal or financial gain.

H. The use of personal information for testing purposes or for training is expressly prohibited. The attached list of authorized test transactions will be used. (See Appendix A)

I. **Password security** - The use of a computer user account when creating or changing any electronic record has the effect of affixing ones signature to it. Therefore, using another's computer user account and password is tantamount to **forgery**.

Providing or allowing any computer account password to be used by any person other than for whom it was created, or using the computer account password of another person, regardless of rank or assignment is **expressly prohibited**. This pertains to:

- City of Dayton network (aka Citrix)
- MIS (Management Information System)
- CAD (Computer Aided Dispatch)
- LEADS (Law Enforcement Automated Data System)
- MDT (Mobile Data Terminal)

Any employee, upon discovering that their password has been compromised, must take immediate measures to nullify the current password.

J. Safeguarding computer accessed information

1. Locking terminals - A computer terminal that is logged on to the city network, MIS, or CAD may not be left unattended unless the user logs off or locks the workstation.

2. Using unlocked terminals - Any employee who finds an unattended workstation that is logged on and not

locked is prohibited from using that device without first logging off the absent user and logging on with their own account. Furthermore, employees finding a terminal in this condition are required to lock the workstation or log off the absent user.

3. Safeguarding information on MDT's – LEADS/NCIC information is often conveyed to police officers using the MDT. Officers will employ measures to prevent unauthorized personnel from viewing their MDT display screens, especially when CJIS information is involved.

   - Mask the screen from view of persons seated in the cruiser.
   - Do not allow persons to look into the cruiser at the display screen.
   - Clear the screen after viewing the information.
   - Lower the screen when leaving the vehicle.

K. All inquiries submitted to LEADS from the MIS system and MDTs will include the driver license number of the person submitting the inquiry. All sworn personnel and all civilian personnel who have LEADS access (Auto Recovery, Radio Information Operators, Data Prep) must enter their driver's license number in a field that has been established in their MIS "home page". Civilian personnel who do not have a driver license will be assigned a number by LEADS Control. Obtaining this number must be coordinated through our LEADS Terminal Agency Coordinator (TAC).

Appendix A.

TEST RECORD INQUIRIES

THROUGH NCIC

Refer to NCIC manual for test records.

THROUGH LEADS

Vehicles

LIC/TST0001 through TST0069

Driving Records

SOC/10000004

OLN/ZZ000007
OLN/ZZ000015
OLN/ZZ000083

BMV Image Records

OLN/ZZ000007
OLN/ZZ000520

THROUGH BCI&I

NAM/PUBLIC,JOHN Q. SEX/M RAC/W DOB/121146

BCI NUMBER/A123456