	LANE COUNTY SHERIFF'S OFFICE POLICY	Number: **G.O. 5.09**
		Issue Date: March 21, 2005
		Revision Date: November 2, 2005; June 6, 2016
CHAPTER: Fiscal Management and Agency-owned Property		Related Policy: APM Chap 1, Section 22, Issue 1 (Personal Use of County Computer Resources); CJIS Security Policy Version 5.4
SUBJECT: CJIS Security Compliance/Use of Computers		Related Laws:

POLICY: In support of Lane County Sheriff's Office's (LCSO) mission of public service to the citizens of Lane County, LCSO provides the needed technological resources to personnel to access FBI CJIS systems and information. All agency personnel with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI (RMS/JMS/CAD) have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of information.

RULE: Computers shall only be used for Sheriff's Office and/or County purposes in accordance with procedures detailed in this General Order and the County Administrative Policies Manual. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDCs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/JMS/CAD, operating systems etc. used to store and/or transmit FBI CJIS is a privilege allowed by LCSO, the State CJIS Security Office for LEDS (CSO) and the FBI. To maintain the integrity and security of LCSO and FBI CJIS systems and data, this computer privilege requires adherence to relevant federal, state and local laws, regulations and contractual obligations. LCSO maintains final authority on all policy and procedural decisions related to information systems containing CJI. All existing laws and LCSO General Orders and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

PROCEDURE:

I. Computer Use

Unless otherwise specified by initial agreement, all programs, documents, and data generated and/or residing on the County computer equipment or generated by County employees using County computers for County program activities are County property.

A. Applications

1. The applications (i.e. software, programs) are County property. The purpose of these applications is to assist employees in conducting County business.

2. The employee's supervisor may authorize limited personal use as long as it does not interfere with County business.

3. Personal use may be cancelled by the employee's supervisor at any time and restricted to County business only. In these instances, the restrictions will be documented in memo form and given to the affected employee.

4. All documents produced on County computers are County property. All documents that are produced on a County computer should be professional as they are public record and may be viewed by the general public.

B. Mail (Outlook)

1. The purpose of the County's email system is to assist employees in conducting County business.

2. All email containing CJIS information must be sent via encryption. Until such time as LCSO has email encryption in place, except in exigent circumstances, sending unencrypted email containing CJIS information is prohibited.

3. Minor and incidental personal use of the email system is authorized as long as it does not interfere with County business.

4. Incidental personal use may be cancelled by the employee's supervisor at any time and restricted to County business only. In these instances, the restrictions will be documented in memo form and given to the affected employee.

5. Emails produced on County computers are County property and are public record. The general public can view these emails at any time. Therefore, messages an employee believes are private or personal may be viewed by the public.

6. Email is a form of communication; therefore, the Sheriff's Office Harassment policy is in force.

C. RMS/JMS/CAD/WebLEDS Systems

1. The sole purpose of the listed systems is to assist employees in conducting County business.

2. Any other use is prohibited.

D. Internet

1. The purpose of the Internet is to assist employees in conducting County business.

2. Internet usage during work hours other than breaks and lunches is allowed only as it relates to work assignments. Internet usage during breaks and lunches must follow the provisions of the APM.

E. Intranet

1. All Sheriff's Office employees have access to the Intranet, which allows access to some sites that are on the Internet as well.

2. The purpose of the Intranet is to assist employees in conducting County business.

3. The Intranet shall not be used to gain access to sites that are not related to the employee's work assignment.

F. Firewalls

1. The purpose of the firewall is to protect County property and allow only authorized employees access to the Internet.

2. Employees attempting to disable the firewall in any way, or obtain a password from authorized employees that have Internet access, to gain Internet access themselves is prohibited.

G. Installation of Software/Hardware

1. Installation of any non-CJI software, programs, or hardware by Sheriff's Office employees is prohibited unless instructed or permission is granted by Lane County Information Services. All CJI software will be authorized by appropriate LCSO staff.

H. Passwords

1. All Sheriff's Office employees that use computers have domain passwords and most staff have other passwords allowing access to CJIS systems, including RMS/JMS.

2. The protection of a password is the employee's responsibility.

3. Employees who use common area computers will lock their computer when away from it and will log off when they leave their terminal at the end of shift.

4. Employees who leave their terminal and do not lock or log off may be subject to discipline for any violation of the above policies that occur while logged on.

5. An employee is prohibited from sharing their password with any other person.

I. Reporting Problems/Errors

1. Sheriff's Office employees should not attempt to fix problems with the computer themselves unless the problem is minor in nature and can be easily rectified (font size, adding a user profile to Outlook).

2. All problems that relate to EIS systems or WebLEDS should be reported to the LCSO application managers (currently the Communications/Records Supervisors and Support Services Manager).

3~~2~~. All other problems should be reported to LCIS by contacting the IS Help Desk by telephone during their working hours. During off-hours, employees should report the problem to a Communication/Records Supervisor or the Support Services Manager to determine if it fits the established callout criteria. If it does not, a ticket should be opened via the IS Service Request form on the Intranet. Employees should be prepared to provide their unique computer terminal number.

II. Disciplinary Policy:

A. Misuse of computing, networking or information resources may result in temporary or permanent restriction of computer privileges up to employment termination. In some situations, account privileges will be suspended to prevent ongoing misuse while under investigation.

Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), per the FBI, the evidence shall be collected, retained, and presented to conform to the rules laid down in the relevant jurisdiction(s). Complaints alleging misuse of LCSO computing and networking resources and FBI CJIS systems and/or data will be directed to those responsible for taking disciplinary action.

Examples of misuse with access to FBI CJIS include:

1. Using a login that you are not the owner of.

2. Leaving the computer logged in with your login credentials unlocked in a physically unsecure location.

3. Allowing an unauthorized person to access FBI CJI (Criminal Justice Information) at any time for any reason. *Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.*

4. Allowing remote access of LCSO issued computer equipment to FBI CJIS systems and/or data without prior authorization by LCSO.

5. Obtaining a computer account that you are not authorized to use.

6. Obtaining a password for a computer account of another account owner.

7. Using LCSO's network to gain unauthorized access to FBI CJI.

8. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.

9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.

10. Violating terms of software and/or operating system licensing agreements or copyright laws.

11. Duplication of licensed software, except for back-up and archival purposes that circumvent copyright laws for use in LCSO, for home use or for any customer or contractor.

12. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with LCSO's network performance.

13. Using electronic mail or instant messaging to harass others.

14. Masking the identity of an account or machine.

15. Posting materials publicly that violate existing laws or LCSO's Code of Conduct.

16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.

17. Using LCSO's technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.

18. Unauthorized possession of, loss of, or damage to LCSO's technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.

19. Maintaining FBI CJI or duplicate copies of official LCSO files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.

20. Using LCSO technology resources and/or FBI CJIS systems for personal or financial gain.

21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy or any other LCSO General Order or the APM.

22. Using personally owned devices on LCSO's network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally owned devices should not store LCSO data, state data, or FBI CJI.

B. The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by LCSO on a case-by-case basis. Activities will not be considered misuse when authorized by appropriate LCSO officials for security or performance testing.

III. Privacy Policy:

A. All agency personnel utilizing agency-issued technology resources funded by LCSO expressly acknowledges and agrees that such service, whether for business of personal use, shall remove any expectation of privacy. Use of LCSO systems indicates consent to monitoring, logging and recording. LCSO reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit and at end of life. LCSO personnel shall not store personal information under the control and management of LCSO with an expectation of personal privacy.

IV. Personal Use Of Agency Technology:

A. Refer to APM Chap 1, Section 22, Issue 1 (Personal Use of County Computer Resources).

V. Misuse Notification:

A. Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, LCSO shall:

1. Establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities;

2. Track, document, and report incidents to appropriate agency officials and/or authorities. Information Service Officers (ISOs) have been identified as the point of contact on security-related issues for their respective agencies and shall ensure that Local Agency Security Officers (LASOs) institute the CJIS System Agency (CSA) incident response reporting procedures at the local level.

B. All LCSO personnel are responsible to report misuse of LCSO technology resources to appropriate LCSO officials.

1. Terminal Agency Coordinator (TAC): LCSO Support Services Manager

2. Agency Coordinator (AC): LCSO Support Services Manager

3. Agency Information Security Officer: LCSO Support Services Manager

4. Local Agency Security Officer (LASO): LCIS Director or designee

5. State-Contact-CSO ISO: OSP CJIS Technical Auditor