


## M1110 – Use of Information Systems and Communication Devices

Effective Date: 08/15/23		Number: M1110
Note: Travelers Papillion APD	CALEA Standards Addressed: 11.4.4, 82.1.6 Nebraska Crime Commission (N.C.C.) O2.4	
Issued By:	Chief Philip D. Lukens	Signed: 

### I. POLICY

It is the policy of the Alliance Police Department that department personnel utilize accessible information and city-owned communication devices for official city and police department business. The internet and any other medium of electronic communication shall not be used in a manner which is detrimental to the mission and function of the department and city. Any exception must be approved by the Chief of Police.

### II. PURPOSE

The purpose of this policy is to provide direction for all employees with respect to the use of our city-owned information systems, land-line and cellular telephones, and any other communication devices used as a medium of communication. (N.C.C. O2.4)

### III. PROCEDURE

#### A. Information Systems Authority

1. Responsibility for the administration and maintenance of the current information system shall be delegated through the Chief of Police, and the Administrative Services Commander. The Department contracts with Bytes for maintenance and upkeep of most network and computer-based information systems.
2. The Administrative Services Division shall maintain oversight and safeguards for all servers which preserve and file official department information, including network, in-car video, building monitoring, access controls, and interview and interrogation records.
3. In the event of major failure of the network system, representatives of Bytes shall be contacted through the paging system or dispatch center. Minor problems encountered with any facet of information systems shall be routed through the chain of command to the Administrative Services Commander.

#### B. Individual Responsibility and Operation

1. All members of the Alliance Police Department shall be issued individual passwords to access the information system network. Confidentiality in password use is required. Any time a department member uses a computer, they shall log on using their name and password. When completed, they shall log off. Any failure to do so may result in disciplinary action. All employees will keep their individual passwords secure. Bytes, in conjunction with the Administrative Services Commander, will conduct an annual audit of passwords to assure there were no breaches of security. Bytes does not maintain a list of passwords;

however, they have the ability to access all information on city-owned systems at the direction of command staff. (CALEA 82.1.6d)

2. All members of the Alliance Police Department shall have a home directory established on the network in their name. All information desired to be saved by officers shall be recorded only on their home directory One Drive. Shared files shall be recorded on the S:/ drive. Although individual employees are authorized to create sub-files within their own home directory, only the authorized Bytes personnel or the Chief of Police may modify/change all other department network directories.
3. No software or program shall be added to the Network System at any time without the permission of the Chief of Police or their designate. When authorized, software will be installed as directed by Bytes, or command staff personnel. Media storage disks (i.e. thumb drives) are provided to all personnel. The use of any outside storage data disk will be authorized only by the Administrative Services Commander. (CALEA 11.4.4)
4. Off-duty F.O.P. Lodge 51 members may utilize a department computer for lodge use if it does not interfere with an on-duty employee's need and must comply with all other requirements as outlined in this order.
5. Use of the Internet should be restricted to accessing sites which provide professional data and information necessary to the performance of one's duties. Any misuse of the Internet may result in restricted individual access. Employees shall not download or upload any information to the system which can compromise the security of the system. The city may install filtering programs to prohibit access to certain unauthorized sites. Special permissions may be granted to certain users for investigative purposes. If enacted, users will be notified of the implementation of filtering software.
6. Any employee accessing an internet site which contains lewd, offensive or other material generally considered pornographic or inappropriate in nature will face disciplinary action. Such administrative action will be severe and may include termination of employment for a first offense violation. We will maintain a work environment which is neither hostile nor offensive and free from any type of sexual harassment, implied or otherwise.
7. In cooperation with Bytes personnel, command staff officers may review, on a regular basis, cache files which are created solely for the purpose of monitoring individual employee Internet usage. Any violations by employees regarding inappropriate internet usage within this order or any general order of the department will result in disciplinary action, up to and including termination.
8. Microsoft Outlook is the official department email software program. All emails transmitted to or from city owned computers are considered public property and may be subject to release through a freedom of information request. It is imperative that all employees conduct themselves as if all emails are at all times under public scrutiny. Unsolicited inappropriate emails received should be immediately deleted and never forwarded to others. Unofficial correspondence captured by installed anti-spam software should be deleted on an ongoing basis. The creation and sending of inappropriate emails will be cause for disciplinary action, up to and including termination.

C. Telephone Usage

1. Telephones, including wired (desk/VOIP lines) and cellular/smart phones issued by the department and paid for by the city are, like other city assets and services, intended for use to conduct city business. When issued, the users of such phones shall have no expectation of privacy. Monthly invoices record the numbers of all calls made and taken and are reviewed by the Chief of Police. If issued a smartphone, tablet or other communication device, all text and/or internet/data usage is also subject to review. City-owned communication devices are only issued for certain positions to conduct department business as a necessity, not a convenience.
2. The department recognizes that there may be occasions when personal calls must be made or received during business hours. Such calls must be kept to a minimum and must not interfere with the employee's work, regardless if the call is made or taken on a city or personal phone. Employees are encouraged to make such calls during authorized breaks.
3. Widespread public service messages deplore distracted driving. Although not illegal, many citizens perceive that a police officer's use of a phone while driving is unprofessional and hypocritical. While on-duty and driving a department vehicle, employees are strongly discouraged from taking or making telephone calls, except when a defensible and justifiable duty-related reason exists. Officers should first move to a safe and stationary location before making or taking a call when possible, and should also expect intense scrutiny when using a phone while driving. Under no circumstances are officers permitted to text while operating a department vehicle.
4. Department members are required to download and maintain required app's to include Intrepid, Field Ops, and Evidence Based Playbook etc. Maintain includes keeping the GPS function active.

D. Terminal Agency Coordinator and Local Agency Security Officer

1. The Alliance Police Department shall appoint a qualified employee to serve as the Terminal Agency Coordinator and Local Agency Security Officer. This person will serve as the point of contact between the Alliance Police Department and the channels of the Nebraska State Patrol and Federal Bureau of Investigations for all things pertaining to NCIC and agency security.
2. To facilitate communication between the Alliance Police Department and outside agencies, as well as to establish an initial point of contact for security purposes. To maintain NCIC/NCIS and Security compliance on a state and national standard. To ensure all incompliances are dealt with accordingly and in a timely manner.
  - a. Terminal Agency Coordinator (TAC)
    - i. The TAC is responsible for communication between APD and NSP. The TAC is responsible for all facets of the NCIC/NCIS, maintaining CJI records, managing records, validating records, and maintaining compliance with NSP and FBI standards.
  - b. Records

- i. Maintenance – The TAC officer will review all documents pertaining to the NCIC/NCIS systems and ensure that all proper documentation is in order and a physical copy is stored in a secure location.
- ii. Retention – The TAC officer will ensure they are up to date with record retention periods and remove any items that no longer meet the criteria for entry.
- iii. Validation – The TAC officer will complete monthly validation reports submitted through the NSP CLEIN portal.
- iv. Compliance – The TAC officer will be familiar with all facets of the NCIC/NCIS system and will ensure the department remains in compliance. Any items found to be out of compliance will be addressed by the TAC officer.

c. Audit

- i. The TAC officer is responsible for all NCIC/NCIS audits. The TAC officer will ensure that all paperwork and questionnaires are completed in a timely manner and submitted within the acceptable time frame.
- ii. The TAC will observe a general monitoring of audit logs in the NCIC/NCIS portal to ensure compliance is being met appropriately.
- iii. The TAC officer will maintain a printed Criminal History Log to ensure all criminal history queries are properly documented.

d. Managing Users

- i. The TAC officer will ensure all new employees are properly screened prior to granting access to the NCIC/NCIS system, to include a fingerprint background check.
- ii. The TAC will ensure all qualified personnel are up to date and maintain their certification through NSP sanctions.

e. The TAC will maintain a physical copy of all NCIC/NCIS users' certificates and digital copies entered in Central Square under each user.

f. The TAC is responsible for notifying appropriate agencies when an employee that has been granted access to the NCIC/NCIS system is no longer employed with the Alliance Police Department.

E. Local Agency Security Officer (LASO)

1. The LASO is responsible for maintaining state and federal compliance with all matters pertaining to the security of all items pertaining to CJI security.

a. Audit

- i. The LASO is responsible for completing and participating in all security audits, regardless of the agency of origin (NSP or FBI).

- ii. The LASO will ensure all proper documentation is in order and that all matters of compliance are met.
  - iii. In the event of noncompliance, the LASO will take the steps needed to ensure that compliance is met prior to the audit, or to at least demonstrate that the agency is addressing the items found not in compliance.
- b. Managing Users
  - i. The LASO is responsible for setting new users up with the appropriate clearance in CJIS Security and Awareness, as well as the signing of security agreements.
  - ii. The LASO is responsible for maintaining a current roster of all CJIS certified employees, to include their date of hire, when the last test was taken, and their security level clearance which shall be maintained in Central Square.
  - iii. The LASO is responsible for maintaining a list of all vendors that will have access to secure areas that may cause them to come in contact with CJI, and maintain security addendums with said vendors which shall be maintained in Central Square.
  - iv. The LASO is responsible for the removal of employees that are no longer active employees of the Alliance Police Department; copies of their security agreements will remain on file for the balance of the year their employment ended plus four years.
- c. Security Breaches
  - i. The LASO will be notified immediately of any and all suspected security breaches. From there, the LASO will complete a "CLEIN NCIC SECURITY INCIDENT REPORT" form and submit it to the proper security agency.

F. Mobile Operations Device Security

1. It is the policy of the Alliance Police Department to utilize the IBM Maas360 device software to provide advanced encryption and device security on all APD issued mobile devices.
2. To maintain FBI CJIS compliant safety and security on all APD issued small form factor mobile devices. This policy will enhance FBI CJIS Policy sanctions and will not replace any minimum standards set by the FBI.
3. DEFINITIONS
 

Large Form Factor – vehicle mount or a carrying case and include a monitor with attached keyboard (MDTs/Laptops)

Medium Form Factor – vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard (Tablets)

Small Form Factor –intended for carry in a pocket or ‘holster’ attached to the body (Smartphones)

4. The Alliance Police department will utilize small form factor mobile devices for day to day operations. These devices will be protected using IBM Maas360, following FBI CJIS requirements and will adhere to the following capabilities:
  - a. Remote locking of device
  - b. Remote wiping of device
  - c. Setting and locking device configuration
  - d. Detection of “rooted” and “jail broken” devices
  - e. Enforce folder or disk level encryption
  - f. Application of mandatory policy settings on the device
  - g. Detection of unauthorized configurations or software/applications
5. The mobile devices will be utilized in compliance with all aspects of the APD policy manual, with special attention to this policy. The mobile devices have special access to CJI and will not be used for any reason other than official police-related duties.
6. The APD will not utilize any “rooted” or “jail broken” devices.
7. Devices will be maintained and updated on a regular basis by the user.
8. Any breach of security (accidental or intentional) will be reported to the Local Agency Security Officer immediately for review.

G. Security Breach Reporting

1. An incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. The additional requirements in this policy are intended to be an enhancement to the existing Standard Operating Procedures of the Alliance Police Department. The Alliance Police Department shall adhere, at a minimum, to the FBI CJIS Security Policy. While the Alliance Police Department may augment or increase the standards, it cannot detract from the minimum requirements set forth by the FBI CJIS Security Policy. This also activates the [Continuity Of Operations Plan per O2222](#) and the policies are to operate in tandem.
2. To ensure the Alliance Police Department is prepared to respond to cyber security incidents, to protect APD systems and data, and prevent disruption of

government services by providing the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance. This policy applies to all APD computers systems and any other government computer systems provided to APD for the support of law enforcement and law enforcement activities.

3. Alliance Police Department management along with Information Technology Division or Information Technology vendor shall develop local agency organization and system-level cyber security incident response procedures to ensure management and key personnel are notified of cyber security incidents as required.
  - a. Incident Response for Breach of Security
    - i. If an incident occurs involving any CJI, the LASO shall be contacted immediately. If it is deemed by the LASO to be a security breach of confidential information, a Security Incident Response Form will be filled out and submitted to the CJIS division of the Nebraska State Patrol.
    - ii. All users are responsible for reporting known or suspected information security incidents. All incidents must be reported immediately to the agency LASO.
    - iii. When a CJIS security incident is reported to the agency's LASO, the LASO will document evidence of such breach and attempt to recover missing CJIS to the extent possible.
    - iv. The LASO will determine where and how the breach occurred and identify the source of compromise and the time frame involved. LASO will collect necessary information to complete a Security Incident Reporting Form, and contact FDLE ISO. LASO will also consult with the Chief of Police and appropriate Agency personnel to determine necessary measures to prevent such incidents and protect CJIS information.
4. Personally owned devices, to include cell phones, tablets or any other devices that are owned and maintained by the user, not the APD: Personally owned devices are not allowed to access the Alliance Police Department's network. Therefore, a device that is not owned by the APD shall not process, store, access or transmit CJI.

#### **IV. RECORD OF CHANGE**

08/15/23      III.(D) Terminal Agency Coordinator and Local Agency Security Officer

08/15/23      III.(E.) Local Agency Security Officer (LASO)

08/15/23	III.(F.) Mobile Operations Device Security
08/15/23	III(G.) Security Breach Reporting