RADIO COMMUNICATIONS PROCEDURE

Original Date of Issue	*General Order Number*
December 20, 1989	**89-05**

Effective Date of Reissue	*Section Code*
June 10, 2021	**OPS-01**

Reevaluation Date	*Amends*
June 2024	

C.A.L.E.A.	*Reference*
81.1, 81.2	**(see "INDEX AS:")**

INDEX AS

Clear Text
Communications Procedure
Joint Communications
Use of Radios

PURPOSE

The purpose of this order is to establish policy to address operational procedures with the Joint Emergency Communications Center (JECC).

I. Policy: Radio Communications Procedure

The Iowa City Police and Fire Departments have combined with several area agencies to form the Joint Emergency Communications Center. JECC serves as the emergency communications system for the City of Iowa City. JECC has its own governing body separate from the City of Iowa City known as the Joint Emergency Communications Services Association Policy Board (JECSA). The City of Iowa City shall have two (2) permanent members on the JECSA board.

II. Procedure: General

A. The Support Services Division shall have primary responsibility and control of communications and communication equipment for the department.

B. The department's radio operations will be conducted in accordance with the Federal Communication Commission's (FCC) procedures and requirements at all times. A copy of the FCC's current rules and regulations shall be available to department personnel through JECC.

C. JECC shall provide the Iowa City community with twenty-four (24) hour toll free voice, text and TDD telephone access system for emergency calls for service.

D. JECC shall establish policy for obtaining and recording the following information for each call for service or self-initiated activity:

1. Control number/Call for Service (CFS) number.
2. Date and time of request.
3. When possible, name and address of complainant.
4. Type of incident.
5. Location of incident.
6. Identification of officers assigned as primary and backup.
7. Time of dispatch.
8. Time of arrival.
9. Time of officer return of service.
10. Disposition or status of reported incident.

E. JECC personnel shall be informed of the supervisor or officer in charge and all assigned patrol officers at the beginning of every patrol shift. All officers assigned shall be considered active unless JECC is informed of a change in status.

F. The office of the Chief of Police shall ensure that JECC has an updated roster including telephone contact information for all current department personnel.

G. JECC shall maintain a current plan or data on the following:

1. Maps detailing the department's service area
2. A written procedure and telephone numbers for procuring emergency and necessary external services for the department.
3. A tactical dispatching plan.

H. JECC shall establish an incident interview technique to be utilized by communications personnel when responding to calls for service. The interview shall determine if the call for service is an emergency or non-emergency. Regardless of the type of call, communications personnel shall inform the caller of the department's response to include direct department assistance or referral to another agency or service provider.

I. The department shall maintain victim and witness assistance and referral information on a 24-hour basis through JECC and through personal response by police officers.

1. Communication personnel shall make a determination, based upon the scope of the call for service, if the victim or witness needs direct

emergency medical service (EMS) and/or physical police response or referral. If either the EMS or police are needed, communications personnel will promptly dispatch appropriate personnel. In cases of a referral, referral lists are maintained at JECC and agency contact phone numbers shall be kept updated.

2. To ensure the timely and appropriate attention to needs, Communications personnel and Station Masters shall respond to victim/witness requests for information and/or service including initial and subsequent requests.

3. If physical police response is necessary, the responding officer shall determine whether overt police actions such as written reports, notifications, arrests or transportation are required or if the need exists for other types of assistance or intervention (e.g. contact with Rape Victim's Advocacy Program (RVAP), CommUnity Crisis Services and Food Bank, DVIP, or the Mobile Crisis Unit/CIT).

J. The department provides and utilizes alternate methods of communication to ensure effective, efficient and proper communication between employees. Methods of alternate communication include cellular telephones and email.

1. Upon hire, employees are assigned an email account through the city to be used in day-to-day business operations of the department. Department employees shall adhere to the City of Iowa City email and internet usage policy and procedures.

2. The Chief of Police may assign cellular telephones to employees when a valid mission-related purpose exists. While cellular telephones can be used in lieu of radios and strict adherence of radio procedures is not mandatory, employees must be professional with their communications. Employees that are issued a department cellular telephone shall adhere to the City of Iowa City cellular telephone policy and procedures.

III. Procedure: Recordings

A. All communications occurring on the two-way radio system and any telephone line answered by JECC shall be recorded. The recording system shall allow for the immediate play back of the recording while continuing to record any additional communications.

B. JECC shall establish the manner in which the records are securely handled and stored, and the length that the records are maintained. The procedure for destruction for each record set shall also be defined. All federal and state regulations related to the maintenance of these records shall be followed. All recordings shall be maintained for a minimum of thirty (30) days. A supervisor may request in writing that a specific official recording be maintained for a longer period of time, the request shall identify the time frame to be maintained.

C. Official Recordings: Official recordings are copies of the original recordings maintained and distributed specifically by JECC staff. Request for official recordings should be made, in writing, to the JECC dispatch shift supervisor.

Requests from the department for official recordings shall be made by a supervisor. When appropriate, official recordings shall be entered as evidence. When utilized as evidence in a criminal case, official recordings may be released upon request to the prosecuting attorney's office with jurisdiction. Official recordings entered as evidence shall be released pursuant to records policy and state law as established in chapter 9 section 82.1.1(Records) of the Operations Manual. Official recordings may be released to media and other outside entities upon the approval of the Chief of Police.

D. Recordings shall only be reviewed for official purposes (e.g. procedural review, complaint investigation). When a recording is needed for a complaint investigation that may result in suspension, demotion, or termination, it shall be an official recording as described above.

IV. Procedure: Criminal Justice Information Systems

A. All officers and other employees required to access the Iowa and the National Crime Information Center (NCIC) criminal justice information system shall maintain proper certification as required. The Support Services division shall maintain all needed records to verify employees have met the standards of each system including initial certification, periodic recertification as required, and updating approved user access.

B. Criminal justice information systems contain confidential information. All employees shall be responsible for knowing and understanding the rules and regulations that govern the use and distribution of this information and will be held accountable for failure to comply with said rules and regulations.

C. The Criminal Justice Information Services (CJIS) produces a comprehensive security policy to establish a minimum set of security requirements for access to FBI CJIS division systems and information and to protect and safeguard criminal justice information. The department shall adopt this security policy and shall adhere to the requirements therein. The CJIS security policy shall be provided to all personnel in the appendix of the Operations Manual.

D. The department shall establish the following positions to comply with the CJIS security policy. The positions shall assume all roles and requirements as established in the CJIS security policy.

1. Terminal Agency Coordinator (TAC): The TAC serves as the point-of-contact at the department for matters relating to CJIS information access. The TAC administers CJIS systems programs within the department and oversees the department compliance with CJIS systems policies. The TAC position for the department shall be a designated Station Master.
2. Local Agency Security Officer (LASO): Due to the technical nature of the duties of the LASO, the Department’s System Analyst shall assume this role. The LASO shall have the following responsibilities:

    a. Identify who is using the state of Iowa Technology Services Bureau approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
    b. Identify and document how the equipment is connected to the state

system.

c. Ensure that personnel security screening procedures are being followed as stated in this policy.
d. Ensure the approved and appropriate security measures are in place and working as expected.
e. Support policy compliance and ensure the state of Iowa Technology Services Bureau is promptly informed of security incidents.

V. Procedure: Radio Communications

A. When on duty, all officers shall be assigned a portable two-way radio that allows direct communication with JECC.

B. All police owned vehicles utilized for enforcement activity shall be equipped with a mounted two-way radio system that allows communication with JECC. Exceptions may be granted for vehicles assigned to task force officers as they may be operating under a different communication system or the vehicle may be utilized for undercover operations.

C. Each radio shall have an emergency alarm that when activated will send an alert to communications personnel. The emergency alarm shall be activated by an officer when they encounter a dangerous situation in which they need immediate backup and are unable to communicate due to the situation. When an emergency alarm is activated, communications shall immediately follow their policy and procedures (JECC SOP 6.37). An emergency alarm activated by an officer shall be handled with the highest priority.

D. Each officer shall be assigned a radio identification number to be utilized during all radio communications.

E. When on-duty, patrol officers shall primarily utilize the two-way radio system to inform communications personnel of their status. This allows communications and other officers to remain cognizant of the officer's activity and current status. Officers may also utilize a mobile data terminal or a cell phone to inform communications and other officers of their status. Officers outside of patrol may utilize the two-way radio system when appropriate to inform communications of their actions. All officers shall be required to notify communications personnel of any type of enforcement activity and shall have a two-way radio system immediately accessible when taking action. Officers working covert and undercover assignments are exempt from this requirement.

F. The department uses plain language as their communication protocol. All transmission will be courteous and professional in nature. At no time shall profanity be used on the radio.

G. Employees shall be reminded that all radio communications and mobile data information can become public record according to Iowa Code.

H. Officers shall keep communications advised of their status following their arrival at calls of unknown or possibly dangerous circumstances.

I. Only pertinent or emergency information shall be transmitted on the two-way radio system.

J. Officers shall keep their portable radios on when away from vehicle or station based radios unless the situation warrants otherwise (e.g. bomb threat, officer safety, etc.).

K. Officers shall keep communications aware of their status. This shall include but is not limited to the following:

1. Upon initiating police action.
2. On arrival and at completion of an assignment.
3. During lunch periods and breaks.
4. When out of service for any reason.

L. Officers and communications personnel shall not argue or contest assigned calls.

1. If there is a problem, the involved personnel shall contact their supervisor.

2. When there is an issue that needs corrective action, it shall be handled by the supervisor. Sensitive matters shall be handled over the telephone or in person.

M. Call assignments may be altered by the supervisor based on information, need, and staffing. Officers not specifically assigned to a call shall refrain from including themselves. If further assistance is needed, communications personnel or the supervisor will assign backup units.

N. Officers shall monitor other agencies radio communications as designated by their supervisor while performing routine patrol duties.

O. In the event of a major crime or medical emergency a specific channel shall be restricted to use for that incident. Anytime an officer is responding to a dangerous situation, radio use shall be restricted to emergency communication only. Officers shall notify dispatch when the situation has been resolved so the channel can be cleared for normal traffic. Consideration should be given for the use of an encrypted event channel when possible.

P. Officers shall use the following procedures when stopping a motor vehicle:

1. Upon stopping a vehicle, an officer shall notify communications by giving their radio number and advising “traffic.” They shall stand by until acknowledged by a dispatcher before giving further information.
2. The officer shall then give license number of vehicle, his/her location. The officer may also want to include the vehicle color, year, make, model and number of occupants. Communications shall run a wanted check of the vehicle after being advised of the license number.
3. After making contact with the occupants of the vehicle, if the officer feels the situation is under control, they shall advise communications they are “Code 4” After an officer gives their status as “Code 4” the dispatcher will follow JECC protocol to periodically check his/her welfare.

Q. When an officer anticipates being out of radio contact, they must notify communications of their location and the reason for leaving. Communications must be able to reach the officer at all times. If radio communication is not possible, the officer may utilize a cellular phone to keep communications informed. Officers working covert and undercover assignments are exempt from this requirement, however, they must have the ability to summon assistance from other officers working with them and JECC shall be made aware of the general location and type of the operation.

R. Officers and communications personnel have access to other agencies via statewide LEA, mutual aid, and other local radio channels. Use of other channels by officers shall be limited to emergency or urgent communications. Proper radio procedure shall be followed when using other channels.

S. The department shall maintain a system to insure interoperability between the city of Iowa City radio system and the JECC system.

VI. Procedure: Terminal Access and Server Access Protection

A. All computers that access criminal justice information shall be located inside the Police Department, or inside Police owned vehicles. No computer terminals should directly face a window or opening that will allow the public to view the information displayed on the screen at any time. If visitors are inside the building they should be restricted from viewing any CJIS data on computer terminals or in paper form. Unauthorized users should not be allowed access to any computer that contains or has access to criminal justice information.

B. Computer terminals that are not attended 24 hours a day shall be secured when not in use, computer terminals should be locked and when possible, office doors remain closed and locked when not in use.

C. Mobile computers and laptop computers should always be positioned so that any non-certified personnel will not have access to view information on the screen. No computer terminal should be left open and unattended at any time, locking the desktop should be utilized when leaving the workspace for any reason.

VII. Server Access Protection

Servers that hold Police shared and personal files are located in Tower place. Access shall be gained by a security badge controlled by City of Iowa City ITS. Systems inside the room shall be secured behind a chain link fence to prevent unauthorized access to network gear and hardware. All users with access to the room shall pass either City of Iowa City or Johnson County background check prior to gaining access. Backup tapes shall be locked inside City of Iowa City Information Services Division. All sites shall be monitored by video surveillance.

VIII. CJIS Security Incident Reporting and Handling

A. Assessment of Threat

If the ITS division is notified of a situation that could be a threat to data, physical infrastructure, or user account and which could lead to compromised data they will first asses if the threat has been blocked by security measures currently in place by either software or hardware devices. If the threat is legitimate but blocked and prevented access the user account password shall be changed as a preventative measure and no further action or reporting is necessary.

If the threat has infected hardware inside the Iowa City Police Department and is a credible threat the action steps below will be put into place.

B. Response to Credible Threat

If the threat is deemed legitimate and has infected any hardware inside the Iowa City Police Department the Information Services staff shall do the following:

- Notify the LASO – Systems Analyst for ICPD of the threat.
- Immediately disconnect the affected hardware from the City of Iowa City network.
- Reset the user account as a preventative measure.
- The affected hardware in use at the time will be examined to try and determine the source or reason for the threat.
- A report will be provided by Information Services to be kept on file by the LASO.

When the review is complete it will be determined if the hard drive needs to be replaced, formatted, or over written. Once that process is completed the machine will be imaged with a standard and tested OS. Virus scan definitions and necessary updates to the hardware will take place and the hardware will be returned to service.

The only variation to the above process is the VMware view environment. It utilizes a non-persistent desktop environment so every time that user logs out of a machine the operating system is destroyed and a new machine is created. This removes the concern of a machine that has been compromised lingering for an extended period.

If there is a chance that malicious code was used to access sensitive data, the LASO will contact the Iowa Department of Public Safety to notify them of the event.

IX. Procedure: Mobile Computers

A. The mobile computer supplements the existing JECC two-way voice radio system. The mobile computer is not intended to replace two-way voice radio communications. The mobile computer is intended to be used for sending and receiving information, making and/or receiving routine inquiries and receiving supplemental information, thus allowing the voice channels to be more available for high priority traffic. The mobile computer may also be used to access the department's records and CAD systems.

B. Department personnel using the mobile computer shall be aware that messages sent on the system may be public records according to Iowa state law. Messages shall be restricted to business use. No personal messages shall be sent. No

obscene, improper, or off-color language will be used in the messages. Officers shall not allow unauthorized users to access their mobile computers.

C. It shall be prohibited to do any of the following actions on the mobile computer:

1. Send messages that may be construed as threatening or intimidating.
2. Unless it is incidental to an investigation, or as part of an official inquiry/response or report, send images that contain nudity, or to send images or words of a sexually suggestive nature, even if the recipient has consented or requested such material.
3. Send jokes or comments that tend to disparage a person or group because of race, ethnicity, national origin, religion, gender, sexual orientation, age, or mental or physical disability.
4. Send messages in any other inappropriate manner.
5. Use another employee's computer ID and password.

D. All usage of the mobile computer to access the IOWA or NCIC systems will be governed by the IOWA and NCIC system's rules and regulations.

E. Any installation of software or modification of existing software on the mobile computer shall adhere to the City of Iowa City ITS policies.

F. All calls for service shall be dispatched by voice and may also be sent by computer. Mobile computers shall be utilized by officers for inquiries, to send administrative messages, to complete needed reports, or to access and update the Department's records and CAD systems.

G. Officers should perform their own status changes (arrive, busy, available, complete) on their mobile computer. They will continue to use the radio system to alert other officers and supervisors of their change in status.

H. All officers should query their own driver license, registration and warrants unless circumstances require a verbal request.

I. When able, officers shall obtain all incident times and numbers by mobile computer. Officer shall be responsible for entering the call narrative and disposition unless unable to do so.

J. When the mobile computer system is down, all activity shall revert back to the two-way voice radio system.

K. Officers shall practice good officer safety techniques. Do not allow operation of the mobile computer to reduce situational awareness, especially in cases involving violators or suspects.

L. Caution shall be exercised when operating the mobile computer when the vehicle is moving. If the operation can be done in a safe manner, an officer may operate the mobile computer while the vehicle is moving. When operation of the mobile computer requires more than a few key strokes or the touching of the computer screen, the officer shall pull over at a safe location to perform the task.

X. Procedure: Response to Calls for Service:

A. One unit will generally be dispatched to handle routine calls for service. The nature of some calls, however, may require additional units for purposes of safety and effectively handling the call. Under most circumstances, two (2) or more units will initially be dispatched in the following instances:

1. Officer calling for help or an activation of an emergency alert.
2. Alarms.
3. Suspicious persons/circumstances.
4. Domestic disturbances.
5. Any call involving a weapon.
6. Crimes in-progress.
7. Any call that poses a risk to the officer.
8. Any call where, in the judgment of a supervisor, additional units are needed.

B. Supervisors may use their discretion when responding to calls; however, there are circumstances that require the presence of a patrol supervisor for the purpose of assuming command. These incidents shall include but not be limited to:

1. Officer calling for help, assaulted, or an activation of an emergency alert (not including false alerts).
2. Death Investigations
3. Natural or man-made disasters.
4. Hostage/barricaded subject.
5. Injured officers.
6. Fatal or potentially fatal accidents.
7. Accidents involving department vehicles or department employees.
8. Incidents where a forced entry is necessary.
9. Vehicle and foot pursuits
10. Shootings or stabbings.
11. Use of Force involving Taser, OC or injury to subject or officer.

XI. Procedure: Entering information into Iowa NCIC systems

A. Station Masters shall be responsible for entry and removal of all information into the Iowa and NCIC computerized data systems for the Iowa City Police Department.

B. When meeting Iowa/NCIC system requirements for entry, officers taking a report in which a vehicle, article, gun, or security have been reported stolen shall request the on-duty Station Master to enter said item. When an item is entered in the Iowa/NCIC system, officers are required to document the entry in the narrative section of the incident.

C. When meeting departmental and Iowa/NCIC system requirements for entry, officers taking a report on a missing person shall be required to immediately forward the information to the on-duty Station Master for entry of the missing person in the Iowa/NCIC system. The on-duty Station Master shall ensure there is an immediate entry into the system.

D. Arrest warrants are entered by a Station Master after receiving them from the

Clerk of Court and the Records Section.

E. When an item or missing person is located and requires removal from the Iowa/NCIC system, the officer responsible for the recovery shall notify the on duty Station Master to remove the entry by providing a supplemental report requesting the removal. The officer shall also submit the supplemental report to the main case file. When the on-duty Station Master is notified by another agency that an item or person has been located, the officer/investigator assigned the case shall be notified and be responsible for producing a supplemental report requesting the removal with copies to the on-duty Station Master and the main case file.

F. On a monthly basis, the State of Iowa shall produce a validation report for the department on all outstanding entries into the Iowa/NCIC system entered for the Iowa City Police Department. On-duty Station Masters shall be responsible for researching said entries for validation. When it is discovered that an item or person is no longer valid for entry in the Iowa/NCIC system, the Station Master shall remove the entry and produce a supplemental report stating it has been removed.

_____

Dustin Liston, Chief of Police

WARNING

This directive is for departmental use only and does not apply in any criminal or civil proceeding. The department policy should not be construed as a creation of a higher legal standard of safety or care in an evidentiary sense with respect to third-party claims. Violations of this directive will only form the basis for departmental administrative sanctions.