

**County Administration Workshop: February 11, 2016**

**9:00 a.m. – Board Conference Room**

Attending: Commissioners Cheryl Walker, Keith Heck, and Simon G. Hare; Terri Wharton, Recorder

Chair Cheryl Walker called the meeting to order at 9:02 a.m.

**1. DEPARTMENT REPORTS & BUSINESS UPDATES**

**A. Public Works**

**1) Warranty Deed between Josephine County and Stephen A. and Mary E. Clarke  
(DeJanvier/Brandes)**

Chuck DeJanvier, County Engineer, explained this property was needed for the McMullin Creek project for the mitigation area required for wetlands and also part of the road right of way. The owners have agreed on the rate of \$17,600 and this is the process of accepting the property. He further explained the County pays roughly 10% of the cost and is reimburse 90% by the federal government. *Staff was directed to place the item on the Consent Calendar on next week's Weekly Business Session Agenda.*

**B. Public Health**

**1) Memorandum of Understanding (MOU) between Josephine County and Shelter Friends (Hoover)**

Diane Hoover, Public Health Administrator, reported the MOU would allow Shelter Friends to receive the adoption fees for adoptions that take place at Petco and PetSmart. She explained Shelter Friends goes to Petco twice a day to care for the cats and provide all of the labor for adoption events. Diane advised after reviewing a 13 week period the average cost would be \$748 plus the two adoption events at PetSmart. She said the budget for the first six months is 83% of projected revenue with expenses only at 33% and said the MOU would only be in place as long as there is a levy in place. *Staff was directed to place the item under Administrative Actions on next week's Weekly Business Session Agenda.*

**C. Department Updates**

**1) Human Resources**

**a. Request for Hiring Outside Policy**

JJ Scofield, Human Resources Director, explained the Sheriff has decided to hire an internal candidate for the Lieutenant position and County promotion policy says the employee receives equal to a 2 step increase. The Sheriff is asking for step 7 instead of step 5 to make up for the increase in insurance premiums going from the Sheriff's insurance plan to the non-union plan. Commissioner Hare recommended step 6 which accommodates the 2 step increase and an additional step to cover additional insurance costs and the Board supported the recommendation. Commissioner Hare felt this was administrative only and didn't need to go to the Weekly Business Session. Commissioner Heck and Commissioner Walker felt it should move forward for transparency. (NOTE: See additional action under Miscellaneous Items). *Staff was directed to place the item on the Consent Calendar on next week's Weekly Business Session Agenda.*

JJ Scofield gave a brief update saying Prothman received 3-4 good quality candidates for the Community Development Director and expects to have more by the end of the week with the first round of interviews beginning on February 28<sup>th</sup>.

**b. Request for FOPPO Contract Approval**

JJ Scofield said the County and FOPPO came to a tentative agreement regarding the contract and without having to go to hearings or arbitration which saved the County money. He advised the changes in the contract were cleaning up some language regarding PTO and OEBS Insurance, a 3% cola year one and two, and internal firearms training provided to the officers. *Staff was directed to place the item under Administrative Actions on next week's Weekly Business Session Agenda.*

**2) Airports**

Larry Graves, Airport Manager, rescheduled to February 18, 2016.

**3) Veterans Services**

Lisa Pickart, Veterans Services Manager, was excused from the meeting. Commissioner Heck said Lisa Pickart was involved with the Music Therapy Program and informed him that Veterans Services continues to be very busy.

**2. FINANCE REPORT & BUSINESS UPDATE**

Arthur O'Hare, Finance Director, advised the IRS would be doing a 2013 payroll audit in the middle of March and it will involve Human Resources and Finance. He said ADP was the payroll company in 2013 so they will prepare all the documents and it should be fairly straight forward.

Arthur reported he would be on vacation from February 15 – 26, 2016.

Arthur said Finance was moving forward on the electronic timesheets meeting with the provider and looking to choose one or two departments to implement the system and then move out from there. He explained it won't be a huge time savings to small departments but would save time in the overall payroll process and provide better employee tracking.

Arthur distributed **Exhibit A – Budget Directives/Goals/Calendar** advised he would be finalizing the budget memo sent to department managers by February 12<sup>th</sup> and the budget directives are straight forward and similar to last year. He said Finance was looking at a status quo budget and the second Secure Rural Schools payment should be received soon. Arthur recommended the Internal Service Fund (ISF) remain the same at 10% and Fleet is saying everything can stay status quo. He had discussion with Ryan Johnson, Building Maintenance Manager, regarding increasing the cost from \$.61 per square foot to \$.65 and or start with \$.61 this year phasing in \$.01 each year. The Board agreed to phase in the increase starting with \$.61 this year. Commissioner Hare explained that Ryan Johnson has no control over his budget such as weather, use of electricity, etc. and the back stop for Facilities is the General Fund. Arthur said he would like to send out the proposed Budget Calendar and the Budget Committee will approve the dates during their first meeting.

Arthur said he would contact Mr. Welsh the new Budget Committee member and give him general information regarding the role and purpose of the Budget Committee.

Commissioner Hare reported he met with Dave Streeter, Forestry Program Manager, and discussed strategy regarding providing a sustainable yield for the coming years.

3. **BOARD BUSINESS:** (ORS 192.640(1) “. . . notice shall include a list of the principal subjects anticipated to be considered at the meeting, but this requirement shall not limit the ability of a governing body to consider additional subjects.”)

**A. Approval of Final Plat Map of Summerfield Estates Phase 2 off of Redwood Highway**

Commissioner Hare made a motion to approve Final Plat Map of Summerfield Estates Phase 2 off of Redwood Highway, seconded by Commissioner Heck. Upon vote, motion passed 3-0; Commissioner Hare – yes, Commissioner Heck – yes, and Commissioner Walker – yes.

**B. Resolution No. 2016-015; In the Matter of a Reappointment to the Emergency Medical Services Board**

Staff was directed to place the item on the Consent Calendar on next week’s Weekly Business Session Agenda.

**C. Resolution No. 2016-016; In the Matter of an Appointment to the Illinois Valley Airport Advisory Board**

Staff was directed to place the item on the Consent Calendar on next week’s Weekly Business Session Agenda.

**D. Matters from Commissioners**

Commissioner Hare advised Jim Brumbach has resigned from the Rural Planning Commission. Staff was directed to appoint John Chambers to Jim Brumbach’s unfilled position.

Commissioner Hare suggested the Board schedule a General Discussion to talk about the Ballot Advisory Question. Staff was directed to schedule it for the February 16, 2016 General Discussion.

Commissioner Hare questioned procedural timelines/issues with the Sunny Valley Sand and Gravel Ordinance and said he would like a weekly update from Legal Counsel and Planning and Commissioner Heck agreed. Commissioner Walker said she would follow up with Legal Counsel.

Commissioner Walker advised the Goal Setting Session at 1:30 p.m. that afternoon was for the Board to set 8-12 goals/projects to be address for 2016-17. Commissioner Hare said he would like to set another Goal Setting Session for individual departments.

**Liaison Update**

Nothing reported.

**E. Miscellaneous Items**

Commissioner Walker said she asked Jenny Hall, Emergency Services Manager, to attend the meeting to discuss some projects she’s been working on.

Jenny Hall discussed the Continuity of Operations Planning (COOP) Preparation Package (**Exhibit B**) and said the State signed the contract and chose the “Gold Planning” so now it’s time to roll out this process. She asked the Board for support to gather information from Department Managers and the Board agreed to support her moving forward with the COOP.

Jenny Hall distributed **Exhibit C – IPAWS Emergency Notification System** and discussed it with the Board. She explained the current alert system allows for Emergency Services to alert small portions of citizens and this program would be able to notify the entire County and said the Board would need to sign the Memorandum of Agreement with FEMA (**Exhibit D**). Commissioner Walker said Jenny has already been trained in using the system and suggested Kory Krauss, Deputy Sheriff/Search and Rescue Coordinator, attend training to be the backup person. *Staff was directed to place the item under Administrative Actions on next week's Weekly Business Session Agenda.*

Commissioner Hare advised he just received an e-mail from the Sheriff regarding the Lieutenant position and explained why the current hiring system doesn't work in regards to the negotiation of salaries. The Board authorized Commissioner Walker to negotiate the position.

Commissioner Hare discussed the court hearing on SB 838 scheduled on February 18, 2016 and said he was advised by staff it was on both his and Commissioner Heck's calendar. The Board agreed Commissioner Heck would attend the hearing.

Commissioner Walker mentioned she has to leave the February 10, 2016 Weekly Business Session at 10:10 a.m.

Meeting adjourned at 10:22 a.m.

**EXHIBITS:**

**Exhibit A – Budget Directives/Goals/Calendar**

**Exhibit B – COOP**

**Exhibit C – IPAWS Emergency Notification System**

**Exhibit D – Agreement with FEMA**

EXHIBIT A  
admin  
2/11/16

# Josephine County, Oregon



## Finance Office

Josephine County Courthouse  
500 NW 6<sup>th</sup> Street / Dept 4, Grants Pass OR 97526  
(541) 474-5255 / FAX (541) 474-5258 / TTY (800) 735-2900

February 4, 2016

To: Board of County Commissioners

From: Arthur O'Hare, Finance Director/Budget Officer

Re: Proposed Budget Calendar for FY 2016-17 Budget

- |                      |   |
|----------------------|---|
| February 16, Week of | Personal Service Worksheets to Departments                          |
| February 22, Week of | Rates for ISF, BOM, Insurance, Fleet to Departments                 |
| March 11, Friday*    | Completed Budgets to Finance  |
| March 28, Week of    | BCC review with Finance and Departments                             |
| April 14, Thursday   | Budget Workshop with Budget Committee, if desired                   |
| April 21, Thursday** | Budget Committee Meeting, 4 to 6 p.m.                               |
| April 28, Thursday** | Budget Committee Meeting, 4 to 6 p.m.                               |
| May 5, Thursday      | Budget Committee Meeting, 4 to 6 p.m.<br>(Approve Budget, Set Rate) |
| May 18, Wednesday    | BCC Budget Hearing on approved budget                               |
| June 1, Wednesday    | BCC Adopt Budget  |

\*After Department review with BCC liaison

\*\*Budget Committee sets meeting times/dates at first public meeting



# Josephine County, Oregon

---

## Finance Office

Josephine County Courthouse  
500 NW 6<sup>th</sup> Street, Dept 4 / Grants Pass OR 97526  
(541) 474-5255 / FAX (541) 474-5258 / TTY (800) 735-2900

February 4, 2016

To: Board of County Commissioners, All Departments

From: Arthur O'Hare, Finance Director/Budget Officer

Re: Proposed Budget Directives/Guidelines for FY 2016-17

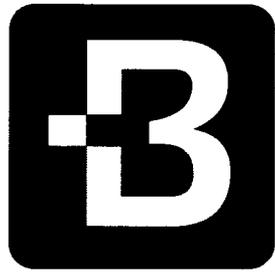
1. Budget will be submitted to Finance by Friday, March 11, 2016.
  - a) **Budgets for FY 2016-17 to be based on FY 2015-16 levels.**
  - b) Budget should be at Service Level 1 (mandatory and/or self supporting). Fund/ Program narratives should address County goals and clearly define program purpose and expected outcomes. Any additions and/or reductions in service level based on revenue sources need to be documented.
  - c) Public Safety Fund budgets and FTE requirements should be based on discretionary monies plus dedicated revenues. Discretionary monies percentage based on FY 2015-16 actual percent allocation after supplemental budget adjustments.
  - d) Funds supported by dedicated monies need to balance revenues with expenditures. All revenue sources must be proven (awarded contracts, grants, etc.) and documented on the Schedule C Appendix Detail form.
  - e) Worksheets, including Personnel Service Schedule D's will be distributed week of February 16. All vacant and new positions need to be added at the end of the schedule and require a "Justification" page with funding source attached. Percentage allocation for positions must be included on Schedule D. FTE's need to be included at Program level.
  - f) Insurance, County Fleet and BOM rates will be distributed week of February 22.
  - g) ISF will be a percentage (10%) based on operational category budgets (Personal Services and Material & Services), shown at Fund level.
  - h) Capital Asset purchases over \$5,000 need to be shown on Schedule F form, including BOM projects.
  - i) Five year projections for capital purchases need to be completed (Charter requirement).
2. General Fund Reserve (Contingency) will be maintained at a minimum of \$3 million dollars.
3. Transfer to Public Safety of \$2.5 million dollars from General Fund resources.

**Josephine County  
Budget Goals  
FY 2016-2017**

**Goals for budget purposes approved 02-04-2016:**

- 1) Improve community outreach and communication to the public by investing in technology that will improve efficiencies within County Departments and provide enhanced service to citizens.
- 2) Develop a sustainable plan for all mandated and essential County government programs.
- 3) Provide access to County services to the citizens of Josephine County in a transparent, open and professional manner.

EXHIBIT B  
Admin  
2/11/16



# **BOLDplanning**

Your Partner in Preparedness



*What's Your Plan?*

**Continuity of Operations Planning (COOP)**

**Preparation Package**

## Table of Contents

INTRODUCTION TO CONTINUITY OF OPERATIONS PLANNING (COOP).....	3
PURPOSE FOR A COOP.....	4
COOP INITIATIVE FOR YOUR ORGANIZATION.....	4
ELEMENTS OF A COOP .....	5
THE PLANNING PROCESS.....	6
SYSTEM ACCESS FOR YOUR ORGANIZATION.....	6
WEB-BASED PLANNING TOOL.....	7
COOP TRAINING.....	7
DATA COLLECTION.....	8
Contacts.....	8
Mission Essential Functions.....	9
Facilities.....	9
Resources.....	10
TRAINING CHECKLIST .....	11
DEFINITIONS.....	12

## **INTRODUCTION TO CONTINUITY OF OPERATIONS PLANNING (COOP)**

*COOP is defined by FEMA (Federal Emergency Management Agency) as an internal effort within individual components of a government to ensure the capability exists to continue essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.*

In the wake of significant events including the September 11<sup>th</sup> Attack, Hurricane Katrina, the Japan Tsunami, and Superstorm Sandy, COOP has become a vital element in emergency planning. Organizations across the country at all levels including federal, state and local have begun preparing for emergencies by engaging their staff and committing the necessary time and resources for developing effective and realistic plans. The federal government has been the leader in this arena and has required all departments to produce COOPs based on published directives and guidance from the Department of Homeland Security. Specific guidance is referenced below.

- Comprehensive Preparedness Guide 101 (CPG 101)  
[http://www.fema.gov/pdf/about/divisions/npd/CPG\\_101\\_V2.pdf](http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf)
- Continuity Guidance Circular 1 (CGC 1)  
[www.fema.gov/pdf/about/org/ncp/cont\\_guidance1.pdf](http://www.fema.gov/pdf/about/org/ncp/cont_guidance1.pdf)
- Continuity Guidance Circular 2 (CGC 2)  
[www.fema.gov/pdf/about/org/ncp/coop/cont\\_guidance2.pdf](http://www.fema.gov/pdf/about/org/ncp/coop/cont_guidance2.pdf)

In order to support the strategic goals for operational continuity, organizations across the country are adopting COOP planning as a high priority. Due to the prioritization by high level management, a COOP program is being developed by your organization to ensure the ability to recover and provide vital services to your constituents following a major disruption.

### **PURPOSE OF A COOP**

Continuity of Operations Planning ensures the ability of an organization to recover and resume operations following a disruption. It is a basic building block of any emergency planning program and is applicable not only in large-scale disaster events or emergencies, but in common non-emergency workplace disruptions as well. Examples might include:

- Facility issues such as an HVAC problem, plumbing leak, or power outage
- Relocation to new office space or the reorganization of divisional units
- Workforce reduction due to illness or absenteeism, loss of key staff due to attrition, or the inability to hire sufficient new workers in a timely manner

It is vital that organizations go through the planning process to develop viable and effective COOPs in order to respond to major disasters, as well as maintain operations during smaller localized disruptions.

### **COOP INITIATIVE FOR YOUR ORGANIZATION**

Your organization has initiated a COOP project to assist all departments with plan development and ongoing plan maintenance. This project is supported by top management within your organization and a core COOP Planning Team has been assembled to support this overall effort. The long-term success of the project depends upon:

- COOP being developed and maintained with a minimal allocation of time and human resources.
- Effective guidance being provided. Many planners will have little or no experience with COOP or emergency planning, and will need support.

COOP consulting and technical support will be available for all planners via telephone and the Internet throughout this planning process.

### ELEMENTS OF A COOP

The elements of a COOP are easily identified, and the process of developing a base plan is relatively simple. In general, a COOP tries to answer basic questions about people, places, and things:

#### Staff Information

- Who are the key people in your organization?
- How are these people organized into teams?
- What are their individual responsibilities?
- If key staff members are unavailable, which individuals are authorized to assume management responsibilities?

#### Facility Information

- *How many different facilities are used by your organization?*
- *What resources and equipment are available and necessary at each facility?*
- *How do you contact and communicate with the facility manager?*
- *If a certain facility were unavailable, where would staff go to resume critical operations?*

#### Resource Information

- *What vital records and systems are required for your organization to provide basic services?*
- *What physical equipment is necessary to perform mission-essential functions?*
- *What communications equipment is available during emergencies?*

By gathering this data during the initial planning process and following up with routine maintenance, an organization can dramatically improve its preparedness.

### THE PLANNING PROCESS

COOP is a team effort. It is designed to ensure that *everyone* is prepared and informed in the case of an emergency, and must involve the entire organization to be truly effective.

- **Executive management** – Provides direction and resources that will successfully develop and maintain the plan. Involvement from the beginning is essential.
- **Managers of key units and departments** – Provide details about their specific staff and operations requirements.
- **Facility managers** – Maintain building operations and relocation options.
- **Information technology managers** – Provide detailed disaster recovery programs for IT infrastructure, and provide support services to other units during disruptions.
- **Staff members** – Those who have key involvement in day-to-day operations can provide details of Mission Essential Functions to the COOP planner.

Depending on the size and complexity of an organization, the COOP team could be as small as four or five individuals. However, for medium and large organizations, many individuals will be actively involved in the ongoing planning process. Most organizations can complete their initial plan quickly with the following estimated time commitments over a 3-6 month period:

- Executive management – 5 hours
- Primary COOP planner – 40 hours
- COOP team member – 15 hours

The actual planning process will consist of four phases:

- **Preparation** – Research and gather existing information within your organization and designate the planning team members.
- **Training and plan development** – Learn the details of a COOP and develop the actual plan through team interaction.
- **Plan review and approval** – Review the draft plan to make sure it is complete and correct before receiving final approval from executive management.
- **Plan maintenance** – Maintain and update the COOP. In order to be useful during a disaster or disruption, the COOP must be kept up-to-date. Part of this routine maintenance effort includes testing, training, and exercising of the plan.

### SYSTEM ACCESS FOR YOUR ORGANIZATION

Each department will have a COOP Planning Team Chief who will act as the primary point of contact for the entire process. Password access will be granted to COOP Planning Team Chief, who can then grant system access to other planning team members. In larger organizations with complex departments or remote locations, it may become necessary for each individual business unit to designate a separate COOP Planning Team Chief, request additional system access, and develop their own unique plan for their operations.

### **WEB-BASED PLANNING TOOL**

The centerpiece of your organization's COOP planning strategy is the BOLDplanning.com web-based COOP system. This system can be accessed through any Internet browser, and uses the latest internet security protocols to safeguard all COOP data.

To log onto the system:

1. Go to your unique website and find the login window in the top left corner
2. Username: Enter the username provided by your project manager
3. Password: Enter the provided password. This is *CASE SENSITIVE*
4. Enter the security code shown in the login window of your computer
5. Click the login button to begin plan development

First time users must enter some basic data for security purposes. The system will prompt you to manage your contact information, customize your Username and Password, and answer two security questions that will be used to verify your identity should you lose or forget your access information in the future.

### **COOP TRAINING**

BOLDplanning offers a comprehensive set of support services to assist departments with the development of COOPs. Along with the web-based tool, BOLDplanning provides:

- Full-day COOP training seminars
- Written documentation and guidance in conjunction with the Web-based tool
- Telephone and Internet support for technical issues or COOP-related questions

The COOP training seminars are hands-on training sessions, and are held at on-site facilities. Each will be held in a computer training facility, and will aid participants as they begin entering their specific plan data.

## DATA COLLECTION

To prepare for the COOP training session, the COOP Planning Team Chiefs should identify critical department staff and instruct them to gather data about their operations. Data for the following elements should be brought to the training session:

### Contacts

The most important aspect of a COOP is related to your staff and being able to communicate with everyone during a disruption. Find your most up-to-date staff roster, and divide them into the following categories:

- **Key staff** – Members that need to respond immediately to support the recovery process.
- **Staff** – All other staff members within your functional unit. These employees will not be required to respond immediately; however, they must be made aware of the situation and any changes to the job location, duties and functions.
- **Non-staff** – Individuals who may not be employed directly by your department but would be contacted in the event of COOP activation (*i.e., security personnel*).
- **Vendor/other** – Vendors may include the armored car service for financial deposits, the locksmith, and others that are relevant to your department's activities.
- **Facilities contact** – Your building contact and/or local contact along with the 24-hour Facilities Support Center number (*TBD*).

For the individuals identified for your COOP Team, you will need the following information:

1. Name (*first, last*)
2. Department/division
3. Job title
4. Work or home address
5. Work, home and cell-phone, pager and fax numbers
6. E-mail address (*if possible, also a personal e-mail address*)
7. Comments – You can add details to the individual's contact information. (For example: *Nurse, or CPR trainer, lives across the street from the main office*, or other details that may be helpful to know at the time of an emergency or during the recovery process.)

### Mission Essential Functions

Identifying and prioritizing Mission Essential Functions is vital to this planning effort. These are not the emergency response functions performed during a certain event; rather, they are the job responsibilities and critical functions performed on a regular day-to-day basis. By outlining all of the normal functions, and the resources and personnel required for these functions, an organization can begin to develop a solid roadmap for recovery. For each function, consider the following factors:

- **Length of disruption** – Determine the length of time that can lapse before each function must be resumed. Certain functions may need to be continued within a few hours of the initial disruption. Others may be able to be delayed for days or even weeks after the event in order to stabilize more critical functions.
- **Prioritization** – Determine how critical each function is relative to the length of disruption above. Additional resources will be allocated to high-priority functions while lower priority functions are put on hold until the situation is stabilized.
- **Required personnel** – Identify the staff required for each function. Give attention to the number of individuals and the type of individuals (*management, technical, administrative, specialized, etc.*) required to perform each function.
- **Required resources** – Identify the resources required to perform each function. It is important to link these resources with each Mission Essential Function.

### Facilities

Gather information about the facilities that support day-to-day operations as well as potential alternate locations that may be used for relocation during disruptions. Most of this data should be readily accessible by contacting the facility manager for your organization.

At least two alternate facilities should be identified for each primary facility in order to support critical operations. Finding and securing an alternate facility may not be feasible for each of your organization's locations; however, it is an opportunity to review your needs and consider possible locations. Talk with your neighbors and identify issues, concerns and needs. Consider the following:

- **"First-choice" facilities** – Locations that can easily support the relocation of your organization. Typically, these are additional facilities managed by the organization that may be geographically close and already have supporting services in place.
- **Regional facilities** – In the event of a large-scale event, first-choice facilities may be equally affected and unavailable. For this contingency, regional options should be determined for relocation.

For each primary and alternate facility, the following elements must be identified:

- Building name and address
- Number of staff at facility (*occupancy number*)
- 24-hour contact information for the facility manager
- Details about building security protocols, including physical security and all access controls
- Details about the communications capabilities within the facility

### **Resources**

Collect information about the equipment, resources and systems that are required to perform the day-to-day activities of your organization. Consider your needs and gather information about the following required resources:

- **Vital records and systems** – Identify all records, systems, files, and documents (*electronic, hard copy, etc.*) necessary for continued operations. Details about the backup procedures for this data are also necessary for your COOP.
- **Required equipment and resources** – Gather information about the required equipment in place in your primary locations, including computers, telephones, office furniture and supplies, and any specialized equipment.
- **Relocation kit items** – Identify specific items in the primary facilities that need to be moved to the alternate location during a disruption.
- **Communications equipment** – Focus on resources used for communicating with staff, related support agencies, the public and local emergency responders.

## **TRAINING CHECKLIST**

You will need the following items for the COOP training session:

### **Contact information:**

Before you arrive, organize your contacts into the key staff, staff, non-staff, vendor, and facilities contacts as identified in the Data Collection section of this document.

- Name (*first, last*)
- Department/division
- Job title
- Work or home address
- Work, home and cell-phone, pager, and fax numbers
- E-mail address (*if possible, also a personal e-mail address*)
- Comments: You can add details to the individual's contact information e.g. Nurse, CPR trainer, lives across the street from the main office, or other details that may be helpful to know at the time of an emergency or during the recovery process.

### **Mission Essential Functions**

- Task list
- Number of employees to complete task (*names or job titles*)
- Time frame during which each function must be completed (*for example, time sheets must be turned in every Friday for payroll, or every Thursday is armored car service pickup*)

### **Facility information:**

- Building location
- Facilities contact
- Business equipment needs (*two computers, service counter, public access, and so on*)

### **Resource Information:**

- Vital records and systems
- Required equipment and resources
- Relocation kit items
- Communications equipment

### **DEFINITIONS**

**Alternate Facility:** A location other than an organization's normal facility used to conduct mission essential functions in the event of COOP activation.

**Continuity Team:** Members of the Continuity Team are responsible for executing the necessary procedures and responsibilities for re-establishing and recovering the operations of the organization's essential functions as identified in Annex C.

**Planning Team:** Members of the Planning Team are responsible for scheduling, conducting and participating in continuity meetings, trainings and exercises; establishing a framework for the organization's continuity plan design and strategy; reviewing the accuracy of the personnel information contained within the plan; and developing an ongoing process for reviewing and updating the plan.

**Continuity of Government (COG):** All measures that may be taken to ensure the continuity of essential functions of governments in the event of emergency conditions, including line of succession for key decision makers.

**Continuity of Operations Plans/Planning (COOP):** Organization's efforts to ensure continuance of essential functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

**Delegation of Authority:** A statement provided to an agency head by the senior agency executive that delegates authority and responsibility. Many agencies require a written delegation of authority to be given to the agency head prior to their assuming command of larger incidents.

**Mission Essential Functions:** An organization's prioritized functions that must be performed under all operational conditions. COOPs are created to ensure that these functions can continue to be performed even following a major disaster.

**Orders of Succession:** The sequence in which one person assumes the roles and responsibilities of a particular function within the organization in the event the usual leadership is unavailable to perform those duties.

**Vital Records:** Records, documents, or other information that, if damaged or destroyed, would cause considerable inconvenience or require replacement or re-creation at considerable expense. These are often records or documents, which, for legal, regulatory, or operational reasons, cannot be irretrievably lost or damaged without materially impairing the organization's ability to continue operations.

# IPAWS Architecture with National EAS

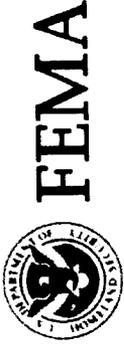
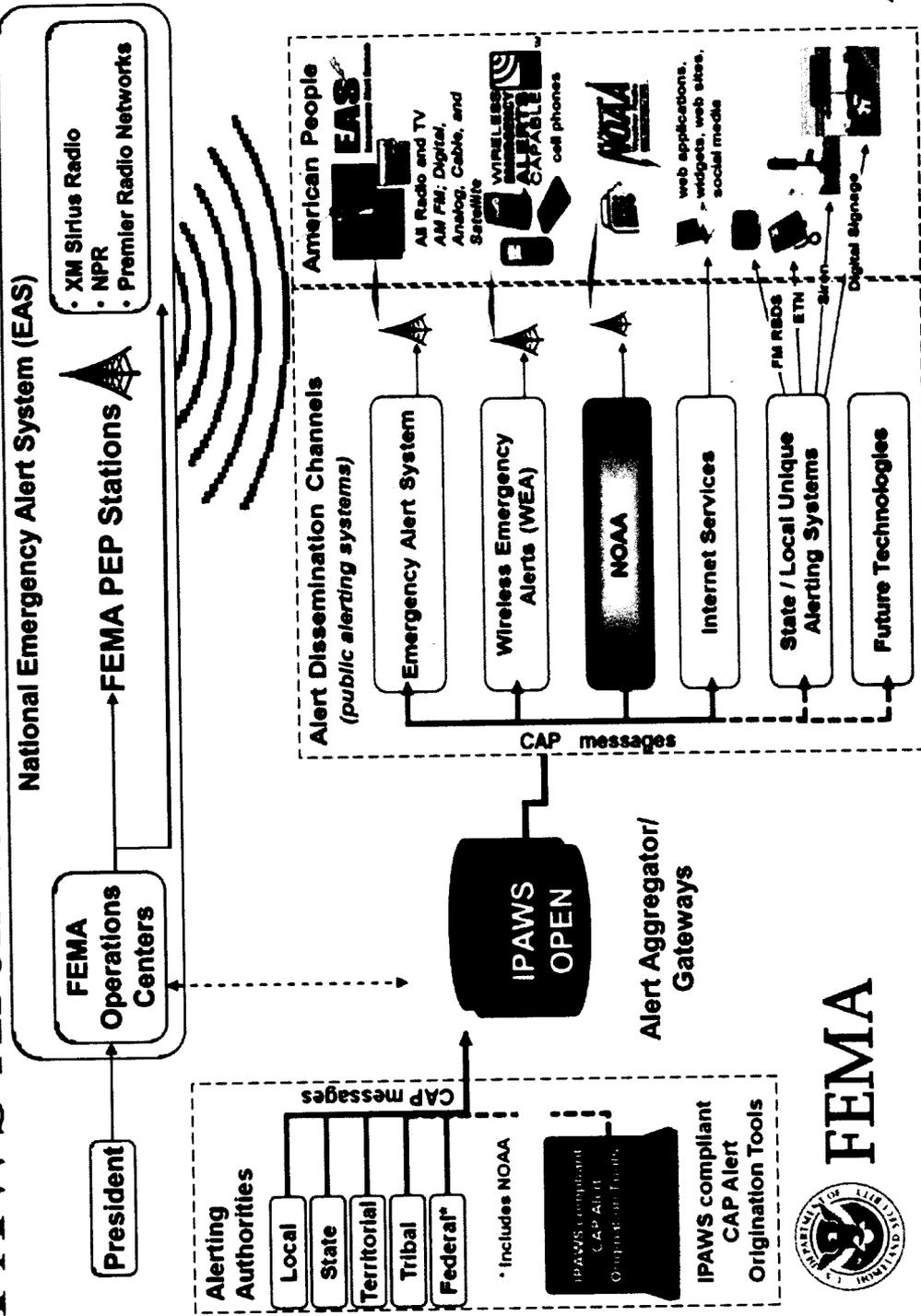


EXHIBIT C  
ADMIN  
2/11/16

EXHIBIT D  
2/11/16  
ADMIN

**Memorandum of Agreement  
between the  
Josephine County  
and the**



**Federal Emergency Management Agency  
Integrated Public Alert and Warning System  
(IPAWS) Program Management Office**

---

**Regarding the use of:**

**Josephine County  
Interoperable System(s)  
and**

**IPAWS OPEN Platform for Emergency Networks  
(IPAWS-OPEN)**

Version 1.1

02 Feb 2016

**WARNING:** This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of the FEMA Integrated Public and Warning System and the FEMA Disclosure Offices.

## MEMORANDUM OF AGREEMENT

**SUPERSEDES: None**

### INTRODUCTION

The purpose of this memorandum is to establish a management agreement between the Josephine County hereinafter referred to as the Collaborative Operating Group (COG), and the Federal Emergency Management Agency (FEMA) IPAWS Division regarding the utilization and security of Josephine County Interoperable System(s) (as shown in Appendix A), which interoperate with the IPAWS Open Platform for Emergency Networks (IPAWS-OPEN). The expected benefit is to enable information interoperability across emergency response organizations and systems as intended by the IPAWS Initiative.

This agreement will govern the relationship between the Collaborative Operating Group and FEMA, including designated managerial and technical staff and system users associated with the aforementioned COG. As indicated within the terms of this agreement, both parties agree to allow system interoperability through the use of SOAP over HTTPS via the public internet. Under this agreement, no direct or networked connection using VPN (or equivalent technology) between the systems named in Appendix A and IPAWS-OPEN is allowed. In the event a direct connection is required, an Interconnection Security Agreement must be executed.

### AUTHORITY

The authority for this agreement is based on the Communications Act of 1934, as amended (47 U.S.C § 606) and the implementation of regulation 47 C.F.R § 11 which establishes the statutory basis under which the FEMA IPAWS Program operates emergency alerting systems. In addition, Executive Order 13407 of June 26, 2006, Public Alert and Warning System Executive Order states, "It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people... establish or adopt, as appropriate, common alerting and warning protocols, standards, terminology, and operating procedures for the public alert and warning system to enable interoperability and the secure delivery of coordinated messages to the American people". In response, FEMA established the IPAWS Program Management Office (PMO) in April 2007.

### BACKGROUND

It is the intent of both parties to this agreement to establish and utilize a standardized web based application interface (as defined by the IPAWS-OPEN Web Service Interface Design Guidance) between the information technology (IT) systems shown below to facilitate the exchange of emergency messages within the production environment. The testing of the interoperability of these systems has been performed through the use of FEMA's Test and Development environment to ensure the transference and receipt of emergency messages using approved messaging standards. The interoperability between these systems is supported by the use of SOAP over HTTPS via the public internet.

### COMMUNICATIONS

Frequent formal communications are essential to ensure the successful management and operation of system interoperability. Both parties agree to maintain open lines of communication between designated staff (as indicated in Appendix B) at both the managerial and technical levels. All communications described herein must be conducted in writing and may be disseminated by electronic means unless otherwise noted.

The owners of the respective systems agree to designate and provide contact information for technical leads for their respective systems, and to facilitate direct contacts between technical leads to support the management and operation of system interoperability. To safeguard the confidentiality, integrity, and availability of the systems and the data they store, process, and transmit, both parties agree to provide notice of specific events within the timeframes indicated below:

- **Security Incidents:** Technical, administrative and/or help desk staff will immediately notify their designated counterparts by telephone or e-mail when a security incident(s) is detected and/or a violation of the Rules of Behavior (see Appendix C) has been identified. Both parties agree to make the appropriate technical and administrative individuals available for all necessary inquiries and/or investigations. Containment and/or resolution procedures will be documented by the identifying party

and after action reports generated and submitted to the system owner and/or designated security officials within five (5) business days after detection of the incident(s).

- **Disasters and Other Contingencies:** The FEMA IPAWS Program Office will notify the COG by telephone, e-mail or other acceptable means in the event of a disaster or other contingency that disrupts the normal operation of IPAWS-OPEN.
- **System Interconnections:** This MOA is intended for systems interoperating with IPAWS OPEN using SOAP over HTTPS via the public Internet. If in the future, an interconnection (i.e. dedicated system-to-system connection) is required to IPAWS-OPEN, this MOA must be updated and an Interconnection Security Agreement (ISA) must be executed. If a change in status from interoperating to interconnected system is required, the initiating party will notify the other party at least 3 months before the planned interconnection is to be in place.
- **Discontinuation of Use:** In the event the use of IPAWS-OPEN is no longer required, the COG agrees to immediately notify, in writing, the FEMA IPAWS Program Office at which time the COGID and associated access credentials will be deactivated.
- **Personnel Changes:** Both parties agree to provide notification of changes to their respective system owner or technical lead. In addition, both parties will provide notification of any changes in the point of contact information provided in Appendix B. All relevant personnel changes and changes to contact information must be provided within 5 business days of the change.

#### **TYPE OF INTERCONNECTIVITY**

Both parties agree that the COG will utilize only the assigned COGID, associated credentials and digital certificates provided by the FEMA IPAWS Program Office to support interoperability between the system(s) listed in Appendix A and IPAWS OPEN. In addition, all interoperable systems must be configured to interface with IPAWS-OPEN over the public Internet using only approved web service standards and associated requirements. A listing of approved web service standards and supporting requirements can be obtained from the IPAWS-OPEN Web Service Interface Design Guidance document.

In the event, a dedicated connection is required, both parties will agree to negotiate and execute an Interconnection Security Agreement (ISA) as required per Department of Homeland Security (DHS) policy which must be signed by all required parties before the interconnection is activated. Proposed changes to either system that affect system interoperability will be reviewed and evaluated to determine the potential impact. If the proposed changes impact the agreed upon terms, the MOA will be renegotiated and executed before changes are implemented.

#### **SECURITY**

To ensure the joint security of the systems and the message data they store, process, and transmit, both parties agree to adhere to and enforce the Rules of Behavior (as specified in Appendix C). In addition, both parties agree to the following:

- Ensure authorized users accessing the interoperable system(s) receive, agree to abide by and sign (electronically or in paper form) the IPAWS-OPEN Rules of Behavior as specified in Appendix C. Each jurisdiction is responsible for keeping the signed Rules of Behavior on file or stored electronically for each system user.
- Utilize FEMA approved PKI certificates to digitally sign messages as they are transported over the public Internet.
- Certify that its respective system is designed, managed and operated in compliance with all relevant federal laws, regulations, and policies.
- Document and maintain jurisdictional and/or system specific security policies and procedures and produce such documentation in response to official inquiries and/or requests.
- Provide physical security and system environmental safeguards for devices supporting system interoperability with IPAWS-OPEN.

- Ensure physical and logical access to the respective systems as well as knowledge of the COGID and associated access criteria are only granted to properly vetted and approved entities or individuals.
- Where applicable, ensure that only individuals who have successfully completed FEMA-required training can utilize the interoperable systems to issue alerts and warnings intended for distribution to the public.
- Where applicable, document and maintain records of successful completion of FEMA-required training and produce such documentation in response to official inquiries and/or requests.

**COST CONSIDERATIONS**

This agreement does not authorize financial expenditures by the COG on behalf of FEMA. The FEMA – IPAWS Division is responsible for the costs associated with developing, operating and maintaining the availability of the IPAWS-OPEN system. The COG is responsible for all costs related to providing their users with access to IPAWS-OPEN via the public Internet. These costs may include hardware, software, monthly Internet charges, completion of security awareness training and other related jurisdictional costs.

**PROPERTY OWNERSHIP**

Each Party agrees and acknowledges that nothing in this Agreement shall be construed as giving a party any proprietary rights in or to the intellectual property of the other party. Each Party further agrees that nothing in this Agreement shall be construed as creating or granting to a party any implied or express license in or to the intellectual property of the other party.

**TIMELINE**

This agreement will remain in effect based on the life of the Authority to Operate (ATO) for IPAWS-OPEN or a maximum of three (3) years after the last date on either signature in the signature block below. Upon expiration of the IPAWS-OPEN ATO or after three (3) years (whichever comes first), this agreement will expire without further action and system access privileges will be revoked. If the parties wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. This newly signed agreement supersedes all earlier agreements, which should be referenced above by title and date. If one or both of the parties wish to terminate this agreement prematurely, they may do so upon 30 days' advanced notice or in the event of a security incident that necessitates an immediate response.

**SIGNATORY AUTHORITY**

I agree to the terms of this Memorandum of Agreement. Noncompliance on the part of either organization or its users or contractors concerning the policies, standards, and procedures explained herein may result in the immediate termination of this agreement.

**Josephine County Official**  
**Name: Cheryl Walker**  
**Title: Commissioner**

**IPAWS OPEN System Owner**  
**Name: Mark A. Lucero**  
**Title: Chief, IPAWS Engineering**

X \_\_\_\_\_  
 (Signature Date)  
**Josephine County**  
**500 NW 6th Street, Dept. 6**  
**Grants Pass, OR, 97526**

\_\_\_\_\_  
 (Signature Date)  
**Attn: IPAWS-OPEN System Owner, Suite 506**  
**Federal Emergency Management Agency**  
**500 C Street SW**  
**Washington, D.C. 20472-0001**

**Federal Emergency Management Agency**

**FEMA CISO or Deputy CISO**

**FEMA Authorizing Official or Designee**  
 \_\_\_\_\_  
 (Signature Date)

\_\_\_\_\_  
 (Signature Date)

## Appendix A

### Listing of Interoperable Systems

IPAWS recognizes that Emergency Management organizations may utilize multiple tools to facilitate the emergency management process. As a result, jurisdictions may need to interoperate with IPAWS-OPEN using more than one system. In order to comply with DHS policy, all systems interoperating with IPAWS-OPEN must be documented and supported by a Memorandum of Agreement. As a result this appendix must be completed to identify all systems associated with the COG and used for interoperating with IPAWS-OPEN. This Appendix must be amended as applicable systems are added or removed from operations.

- **IPAWS-OPEN**

Function:	IPAWS-OPEN is the backbone system that structures the alert and distributes the message from one interoperating and/or interconnected system (message sender) to another interoperating and/or interconnected system (message recipient).
Location:	FEMA Emergency Operations Center
Description of data, including sensitivity or classification level:	Messaging data is considered Sensitive But Unclassified (SBU) information and does not contain Personally Identifiable Information (PII), Financial data, Law Enforcement Sensitive Information or classified information. Each message that flows through the IPAWS-OPEN system will be associated to a specifically assigned system User ID and COGID as captured within the message elements. This information will be retained in system logs.

The systems listed below are managed and operated by the COG and are subject to the terms defined within the Memorandum of Agreement including the Rules of Behavior in Appendix C. Each interoperable system will be assigned unique authentication credentials, which must be protected by the COG. In the event these credentials are compromised, the COG is expected to immediately contact the IPAWS Program Management Office. The systems listed below are only allowed to interoperate with IPAWS-OPEN based on the criteria set forth within the IPAWS-OPEN Web Service Interface Design Guidance.

- **Everbridge Aware, Everbridge Matrix, Everbridge SmartGIS, Everbridge Mass Notification, Everbridge Interactive Visibility**

Function:	Send public alerts for major events for dissemination to CMAS
Location:	Burbank, CA; Denver, CO; Amazon West Northern, CA;
Description of data, including sensitivity or classification level:	COTS FOUO Internet-based SaaS mass notification application. See <a href="http://www.everbridge.com">www.everbridge.com</a>

*\*Add additional tables as needed.*

## **Appendix B**

### **COG Point of Contact Information**

#### **Designated COG Primary Point of Contact:**

**Name: Jenny Hall**

**Title: Emergency Services Manager**

**Business Email Address: jhall@co.josephine.or.us**

**Primary Phone Number: 541-474-5300**

**Alternate Phone Number:**

**Organization: Josephine County Emergency Management**

**Mailing Address: 500 NW 6th Street, Dept. 6, Grants Pass, OR, 97526**

#### **Designated Alternate Point of Contact:**

**Name: Cory Krauss**

**Title: Deputy Sheriff**

**Business Email Address: ckrauss@co.josephine.or.us**

**Primary Phone Number: 541-474-5301**

**Alternate Phone Number:**

**Organization: Josephine County Sheriff's Office**

**Mailing Address: 1901 NW F Street, Grants Pass, OR, 97526**

#### **Designated Technical Point of Contact:**

**Name: Jenny Hall**

**Title: Emergency Services Manager**

**Business Email Address: jhall@co.josephine.or.us**

**Primary Phone Number: 541-474-5300**

**Alternate Phone Number:**

**Organization: Josephine County Emergency Management**

**Mailing Address: 500 NW 6th Street, Dept. 6, Grants Pass, OR, 97526**

## FEMA: Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN)

Contact Name	Contact Number	Email Address	Summary of System Responsibilities
Adrian R. Gardner	202-646-3006	Adrian.Gardner@fema.dhs.gov	Chief Information Officer, FEMA
Gerald Singleton	215-931-5698	Gerald.Singleton@fema.dhs.gov	Acting Chief Information Security Officer
Mark Lucero	202-646-1386	Mark.Lucero@fema.gov	System Owner
Gary Ham	703-899-6241	Gary.Ham@associates.dhs.gov	FEMA PMO - IPAWS-OPEN
Maurice Carter	202-212-4065	Maurice.Carter@associates.dhs.gov	FEMA ISSO - IPAWS-OPEN
Neil Bourgeois	703-732-6331	Neil.Bourgeois@associates.dhs.gov	FEMA-EADIS IPAWS-OPEN Tech Lead

# Appendix C

## IPAWS-OPEN Rules of Behavior

### 1.0 INTRODUCTION

The following rules of behavior apply to all persons with application access to Josephine County Interoperable System(s) and/or who have been issued a COGID with associated credentials for IPAWS-OPEN. These individuals shall be held accountable for their actions related to the information resources entrusted to them and must comply with the following rules or risk losing their access privileges. The Rules of Behavior apply to users on official travel as well as at their primary workplace (e.g., Emergency Operations Center – EOC) and at any alternative workplace (e.g., telecommuting from a remote or satellite site) using any electronic device including laptop computers and portable electronic devices (PED's). PED's include personal digital assistants (PDA's) (e.g. Palm Pilots), cell phones, text messaging systems (e.g., Blackberry), and plug-in and wireless peripherals that employ removable media (e.g. CDs, DVDs, etc.). PEDs also encompass USB flash memory (thumb) drives, external drives, and diskettes. These Rules of Behavior are consistent with existing DHS policies and DHS Information Technology (IT) Security directives and are intended to enhance the awareness of each user's responsibilities regarding accessing, storing, receiving and/or transmitting information using IPAWS-OPEN.

### 2.0 APPLICATION RULES

#### 2.1 Official Use

- IPAWS-OPEN is a Federal application to be used only in the performance of the user's official duties in support of public safety as described in the National Incident Management System (NIMS).
- The use of the IPAWS-OPEN for unauthorized activities is prohibited and could result in verbal or written warning, loss of access rights, and/or criminal or civil prosecution.
- By utilizing IPAWS-OPEN, the user of the interoperable system(s) consents to allow system monitoring to ensure appropriate usage for public safety is being observed.
- EMA's will be held accountable for safeguarding all configuration items and information entrusted to them by FEMA. EMA's are expected to manage the relationship with supporting vendors, consultants and any other entities providing system support on their behalf. In addition, EMA's will be held accountable in the event of a security breach or disclosure of sensitive configuration information such as digital certificates. Each EMA understands that the use of digital signatures used on behalf of the EMA is binding for the EMA and EMA's will be held accountable accordingly. In the event sensitive information is mishandled, utilization of IPAWS-OPEN may be immediately revoked.
- If software interoperating with IPAWS-OPEN enables users to geo-target public alert messages by means of geospatial polygons or circles, then the user shall restrict any such geospatial boundaries so as to remain within the geographical limits of their public warning authority (or as near as possible), as determined by applicable state and/or local laws and duly adopted operational plans.

#### 2.2 Access Security

- All Email addresses provided in connection with interoperable system(s) user accounts must be associated to an approved email account assigned by the user's emergency management organization. The use of personal email accounts to support emergency messaging through IPAWS-OPEN is prohibited.
- Upon approval of the MOA by FEMA, a COG account with COGID and Digital Certificate will be created and issued to the designated technical representative. All individuals with knowledge of these credentials must not share or alter these authentication mechanisms without explicit approval from IPAWS.
- Every interoperable system user is responsible for remote access security as it relates to their use of IPAWS-OPEN and shall abide by these Rules of Behavior.

### 2.3 Interoperable System User Accounts and Passwords

- All users must have a discrete user account ID which cannot be the user's social security number. To protect against unauthorized access, passwords linked to the user ID are used to identify and authenticate authorized users.
- Accounts and passwords shall not be transferred or shared. The sharing of both a user ID and associated password with anyone (including administrators) is prohibited.
- Accounts and passwords shall be protected from disclosure and writing passwords down or electronically storing them on a medium that is accessible by others is prohibited.
- The selection of passwords must be complex and include:
  - At least eight characters in length
  - At least two (02) upper case and two (02) lower case letters
  - At least two (02) numbers and one (01) special character.
- Passwords must not contain names, repetitive patterns, dictionary words, product names, personal identifying information (e.g., birthdates, SSN, phone number), and must not be the same as the user ID.
- Users are required to change their passwords at least once every 90 days.
- Passwords must be promptly changed whenever a compromise of a password is known or suspected.

### 2.4 Integrity Controls & Data Protection

- All computer workstations accessing IPAWS-OPEN must be protected by up-to-date anti-virus software. Virus scans must be performed on a periodic basis and when notified by the anti-virus software.
- Users accessing interoperable system(s) to utilize IPAWS-OPEN must:
  - Physically protect computing devices such as laptops, PEDs, blackberry devices, smartphones, etc;
  - Protect sensitive data sent to or received from IPAWS-OPEN;
  - Not use peer-to-peer (P2P) file sharing, which can provide a mechanism for the spreading of viruses and put sensitive information at risk;
  - Not program computing devices with automatic sign-on sequences, passwords or access credentials when utilizing IPAWS-OPEN.

Users may not provide personal or official IPAWS-OPEN information solicited by e-mail. If e-mail messages are received from any source requesting personal information or asking to verify accounts or other authentication credentials, immediately report this and provide the questionable e-mail to the Local System Administrator and/or the Josephine County Help Desk.

- Only devices officially issued through or approved by DHS, FEMA and/or approved emergency management organizations are authorized for use to interoperate with IPAWS-OPEN and use of personal devices to access and/or store IPAWS-OPEN data and information is prohibited.
- If a Blackberry, smartphone or other PED is used to access the interoperable system(s) to utilize IPAWS-OPEN, the device must be password protected and configured to timeout or lock after 10 minutes of inactivity.
- If sensitive information is processed, stored, or transmitted on wireless devices, it must be encrypted using approved encryption methods.

## **2.5 System Access Agreement**

- I understand that I am given access to the interoperable system(s) and IPAWS-OPEN to perform my official duties.
- I will not attempt to access data, information or applications I am not authorized to access nor bypass access control measures.
- I will not provide or knowingly allow other individuals to use my account credentials to access the interoperable system(s) and IPAWS-OPEN.
- To prevent and deter others from gaining unauthorized access to sensitive resources, I will log off or lock my computer workstation or will use a password-protected screensaver whenever I step away from my work area, even for a short time and I will log off when I leave for the day.
- To prevent others from obtaining my password via "shoulder surfing", I will shield my keyboard from view as I enter my password.
- I will not engage in, encourage, or conceal any hacking or cracking, denial of service, unauthorized tampering, or unauthorized attempted use of (or deliberate disruption of) any data or component within the interoperable system(s) and IPAWS-OPEN.
- I agree to inform my Local System Administrator when access to the interoperable system(s) and/or IPAWS-OPEN is no longer required.
- I agree that I have completed Computer Security Awareness training prior to my initial access to the interoperable system(s) and IPAWS-OPEN and that as long as I have continued access, I will complete Computer Security Awareness training on an annual basis.

## **2.6 Accountability**

- I understand that I have no expectation of privacy while using any services or programs interoperating with IPAWS-OPEN.
- I understand that I will be held accountable for my actions while accessing and using interoperable system(s) and IPAWS-OPEN, including any other connected systems and IT resources.
- I understand it is my responsibility to protect sensitive information from disclosure to unauthorized persons or groups.
- I understand that I must comply with all software copyrights and licenses pertaining to the use of IPAWS-OPEN.

## **2.7 Incident Reporting**

- I will promptly report IT security incidents, or any incidents of suspected fraud, waste or misuse of systems to the Local System Administrator and/or the Josephine County Help Desk.

### 3.0 IPAWS-OPEN Rules of Behavior Statement of Acknowledgement

*I have read and agree to comply with the requirements of these Rules of Behavior. I understand that the terms of this agreement are a condition of my initial and continued access to Josephine County Interoperable System(s) and IPAWS-OPEN and related services and that if I fail to abide by the terms of these Rules of Behavior, my access to any and all IPAWS-OPEN information systems may be terminated and I may be subject to criminal or civil prosecution. I have read and presently understand the above conditions and restrictions concerning my access.*

Name (Print): \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_