This document outlines the response expectations of Yolo County due to Cyber Security.

# Cyber Security Annex

## An Annex to the Yolo County Emergency Operations Plan

Version 1.0 August 2024

# PROMULGATION

This Emergency Support Function Annex to the County of Yolo Emergency Operations Plan describes how Yolo County will manage an emergency incident or disaster mitigation, preparedness, response, and restoration related to this Emergency Support Function. All Primary and Support agencies identified as having assigned responsibilities in this Emergency Support Function shall perform the emergency tasks described, including preparing and maintaining Standard Operating Guidelines and Procedures and carrying out the training, exercises, and plan maintenance needed to support the plan.

This Emergency Annex plan was developed using the Comprehensive Planning Guide 101 version 3 from the Federal Emergency Management Agency and California's emergency planning guidance documents. Adoption will occur following the established maintenance schedule; however, the plan may be modified in the interim without prior approval and formal adoption under the direction of the Director of Emergency Operations. The revised plan will be relayed digitally to all Primary and Support agencies with assigned responsibilities in this Emergency Support Function. The Primary assigned agency will coordinate the review and update of the plan with the Support agencies as needed at least every three years. This Emergency Support Function plan supersedes any previous versions.

This Emergency Support Function Annex applies to Primary and Support agencies within Yolo County who are assigned responsibilities in Section 4.2 Responsibilities by Emergency Support Function of the All-Hazard Emergency Operations Plan and identified within the Emergency Support Function Annex.

This plan replaces previous annexes of the same or similar title.

The County of Yolo Board of Supervisors chairperson will formally promulgate this annex. The County Ordinance empowers the County Board of Supervisors to review and approve emergency and mutual aid plans.

_____ _____

Lucas Frerichs Date:
Chair of the Board of Supervisor

# TABLE OF CONTENTS

# SECTION 1.0: INTRODUCTION

## 1.1 OVERVIEW

A cyber-related incident may take many forms: an organized cyber-attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical infrastructure or key assets. Over the years, these cyber threats have increased in frequency, scale, sophistication, and severity. The ranges of cyber threat actors, attack methods, targeted systems, and victims are also expanding. The United States (U.S.) government's 2018 assessment of the threat environment concluded that the potential for a surprise attack in the cyber realm will increase in the coming years, as more devices are connected to the internet and threat actors grow their attack capabilities. Attack methods such as ransomware and malware have spread globally and can disrupt operations and expose sensitive data to vulnerability.

Large-scale cyber incidents may overwhelm government and private sector resources by disrupting the Internet or taxing critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid threat identification, information exchange, investigation, and coordinated response and remediation are critical in cyber consequence management.

A cyber incident could seriously disrupt reliance on computers and telecommunication networks. Cyber incidents threaten the electronic infrastructure supporting the social, health, and economic well-being of Yolo County's residents. Interlinked computer networks regulate the flow of power, water, financial services, medical care, public safety, telecommunication networks and transportation systems. The consequences could cause significant disruption of operations and economic losses. Cybercriminals also target personal information stored online for use in fraudulent activities. Healthcare, financial institutions and e-commerce are typical targets of criminal data breaches of personal information.

## 1.2 PURPOSE

The purpose of this annex is to facilitate effective and coordinated response and recovery activities with Yolo County stakeholders, state, federal, local and private agencies to minimize the impact of cybersecurity incidents. This Annex discusses organization's actions and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recover from severe or emergency level cyber-related incidents.

This Annex will facilitate, coordinate, and support the following core functions of the ESF:

- Refining inter-agency and cross-sector information coordination, encouraging information sharing, and performing threat analysis
- Sharing information in a way that protects privacy, confidentiality, and civil liberties
- Establishing and maintaining the Incident Response Team (IRT) to detect, report, and respond to cyber incidents.

## 1.3 SCOPE

In the event of a severe or emergency level cybersecurity incident, this annex will provide a centralized framework for responding to cyber-incidents that may involve cyber terrorism, critical infrastructure information systems, technological emergencies, or other emergencies or disasters with impacts on information technology (IT) capabilities, secure data, privacy information within Yolo County. Significant cybersecurity incidents may occur independently or in conjunction with disaster emergency operations, potentially impacting public health, safety, or critical infrastructure.

The Annex provides an organizational structure, roles of responsibilities, concept of operations, annex maintenance information, and operational tools to support operations of this annex. It also provides a means of defining, specifying, and maintaining the functions and resources required to ensure timely and consistent actions, communications, and response efforts before, during, and after an incident with implications related to cybersecurity.

Cyber incidents vary in scale and severity, and stakeholders within this annex will need to respond in proportion to the threat to effectively manage resources and personnel. Table 1 describes the incident severity scale to be used by this annex, including the level of effort and expected coordination with state, local, tribal, and territorial (SLTT) governments and other mission partners.

**TABLE 1: CYBER INCIDENT SEVERITY MATRIX**

| Cyber Incident Severity | Description | Level of Effort—Description of Actions |
|---|---|---|
| **Level 0—Steady State** | Unsubstantiated or inconsequential event. | Steady State, which includes routine watch and warning activities. |
| **Level 1—Low** | Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. | Requires coordination among State Departments and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements. |
| **Level 2—Medium** | May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. | Requires coordination among Victim Departments, Victim Agencies, or SLTT governments due to minor to average levels and breadth of cyber related impact or damage. Typically, this is primarily a recovery effort. |
| **Level 3—High** | Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. | Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of damage. Potential involvement of FEMA and other federal agencies. |
| **Level 4—Severe** | Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties. | Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of cyber impact or damage. Involvement of Federal Partners if needed for incident. |
| **Level 5—Emergency** | Poses an imminent threat to the provision of wide-scale critical infrastructure services, State government security, or the lives of California citizens. | Due to its severity, size, location, actual or potential impact on public health, welfare, or infrastructure, the cyber incident requires an extreme amount of State assistance for incident response and recovery efforts, for which the capabilities to support do not exist at any level of State government. Involvement of Public- Private Partnerships if needed for incident. |

## 1.4 SITUATIONAL OVERVIEW AND ASSUMPTIONS

The response to and recovery from a cyber-incident must consider existing challenges to the effective management of significant cyber incidents and the resulting physical effects and consequences of such cyber incidents. Such consideration allows resources to be appropriately channeled into resolving identified challenges. Assumptions and identifiable challenges include but not limited to:

- Management of Multiple Cyber Incidents: The occurrence or threat of multiple cyber incidents may significantly hamper the ability of responders to adequately manage the cyber incident. Strategic planning and exercises should be conducted to assist in addressing this problem.
- Availability and Security of Communications: A debilitating infrastructure incident could impede communications needed for coordinating response and recovery efforts. Flexible secure, reliable communication systems are needed to enable public and private-sector entities to coordinate efforts in the event that routine communications channels are inoperable.
- Availability of Expertise and Surge Capacity: State, Federal and Local agencies must ensure that sufficient technical expertise is developed and maintained within the County to address the wide range of ongoing cyber incidents and investigations. In addition, the ability to surge technical and analytical capabilities in response to cyber incidents that may occur over a prolonged period must be planned for, exercised, and maintained
- Coordination with the Private Sector: Cyberspace is largely owned and operated by the private sector; therefore, the authority of the Yolo County to exert control over activities in cyberspace is limited.
- A cyber incident may occur at any time of day with little or no warning, may involve single or multiple geographic areas
- This command framework may be utilized in any incident with cyber related issues, including significant cyber threats and disruptions; crippling cyber-attacks against the Internet or critical infrastructure information systems; technologic al emergencies; or declared disasters.
- This Annex describes the specialized application of the National Response Framework (NRF) to cyber-related incidents. These cyber incidents may result in activation of the Cyber Annex and other Emergency Support Function (ESF) annexes.

# SECTION 2.0: ROLES & RESPONSIBILITIES

## 2.1 SITUATIONAL OVERVIEW AND ASSUMPTIONS

As the leading department, Yolo County Innovation and Technology Services (YCITS) will take actions to prepare, within staffing and fiscal constraints, respond to, and recover from all emergencies and disasters impacting the Information Technology (IT) systems and services within Yolo County. Responsibilities include:

- Providing indications and warning of potential threats, incidents, and attacks;
- Information-sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation;
- Analyzing cyber-vulnerabilities, exploits, and attack methodologies;
- Defending against the attack;
- Leading county-level recovery efforts
- Collaborate with YCOES to prepare, respond, and recover from cyber incidents
- Supporting and keeping other ESFs and organizational elements informed of ESF operational priorities and activities

However, during response operations, primary responsibility for implementing tactical activities and remediation will transition to the IRT, while YCOES and YCITS will maintain situational awareness and strategic oversight of the incident. Table 2 defines additional responsibilities for ITS under the incident management phases.

**TABLE 2: YCITS Responsibilities**

| YCITS Responsibilities |
|---|
| **Mitigation** |
| • Oversee the implementation of processes to mitigate against the impacts of cyber incidents, including but not limited to:<br>- Performing recurring data backup<br>- Maintaining off-site data storage<br>- Maintaining awareness of alternate facilities and Point of Contact information<br>- Performing security device configuration reviews<br>• Utilizing the County's Information Security Program to assist in mitigating all types of cyber risks. This program;<br>- Describes the components of the security plan<br>- Describes all associated policy suite to support all activities that must be done to provide the best protections possible |
| **Preparedness** |

| |
|---|
| • Build the county's capacity to collectively respond to cyber incidents<br>- Conduct cybersecurity awareness training and exercises to increase awareness about cyber hygiene and best practices<br>- Conduct cybersecurity training and exercises to continuously validate planning concepts and operations in coordination with YCOES |
| • Establish and maintain working relationships with local, county, state, and federal entities to support the improvement of county's response capabilities and improve coordination |
| • Monitor information and potential threats using multiple information pathways (e.g., Open-Source Intelligence [OSINT], coordination with fusion centers) |
| • Conduct cyclical analysis of risk to assess and achieve operational benchmarks |
| • Develop and revise incident handling and reporting plans, protocols, and policies on a continuous basis, and subsequently publicize those changes with relevant audiences |
| • Identify resources to support incident preparedness, response, and recovery and training stakeholders on available resources |
| • Maintain and train the IRT |
| • Coordinate with YCOES to maintain and update all local, county, state, federal, and commercial contact lists and test contact methods on at least a quarterly basis |
| • Maintain relationships and contact information for all other ESFs. |
| • Maintain the cyber security annex and support an iterative and collaborative planning process |
| **Response** |
| • Schedule an initial conference with the affected entity to assess the incident, classify its severity on the severity matrix, determine the parties needed to support the IRT, and activate the IRT |
| • Develop and employ sufficient methodologies (via a containment plan) to contain the incident in order to minimize continued impact and/or disruption of services while reducing the likelihood of contamination to other services |
| • Continue to gather and analyze information about the incident, in order to evolve the remediation strategy as the incident progresses |
| • Document facts, gather and maintain evidence as needed to support criminal investigations, coordinating with the affected entity for key threat indicators |
| • Detect and triage potential cyber incidents |
| • Notify the YCOES of any changes to the incident severity level for a possible EOC activation |
| • Share information to IRT team members and various intelligence channels |
| • Provide regular briefings or updates to elected officials and/or department leadership |
| • Deploy tactics to contain, eradicate, and recover from a cyber incident |

| |
|---|
| • Ensure confidentiality, integrity, and availability of all information related to the incident |
| • Report incidents using proper incident handling or notification protocols |
| **Recovery** |
| • Execute relevant backup strategies to perform data restoration |
| • Perform after-action analysis, develop an after-action report, and address corrective action items based on the identified root cause |
| • Participate in after action analysis conducted by YCOES |
| • Support damage assessments, as needed |

## 2.2 SUPPORTING AGENCIES

ESF support agencies are those entities with specific capabilities or resources that support the primary agency in executing the cyber security annex mission. When the annex is activated, support agencies are responsible for:

- Conducting operations, when requested by primary agency, consistent with their own authority and resources, except as directed otherwise pursuant to sections 402,403, and 502 of the Stafford Act.
- Participating in planning for short- and long-term incident management and recovery operations and the development of supporting operational plans, SOPs, checklists, or other job aids, in concert with existing first responder standards.
- Assisting in the conduct of situational assessments.
- Furnishing available personnel, equipment, or other resource support as requested by primary agency.
- Providing input to periodic readiness assessments.
- Maintaining trained personnel to support interagency emergency response and support teams.
- Identifying new equipment or capabilities required to prevent or respond to new or emerging threats and hazards, or to improve the ability to address existing threats.

The roles and responsibilities are consistent with those identified in the Yolo Emergency Operations Plan (EOP). The level at which the Emergency Operations Center (EOC) is activated will be based on the situation and the need for a coordinated response to the emergency event. Table 3 illustrates the roles of each ESF during the response operations.

**TABLE 3: ESF Responsibilities**

| Emergency Support Function | Lead Coordinating Agency for Yolo County | Specific Responsibilities during events |
|---|---|---|

| | | |
|---|---|---|
| **ESF #1 – Transportation** | Yolo County Transportation District | • Provide status of all primary and alternate cyber controls and components in Transportation affected by, or affecting response to, cyber incidents<br>• Coordinate during cyber incidents impacting traffic monitoring systems, industrial control systems, and geographic information systems (GIS)<br>• Conduct global positioning system (GPS) tracking and monitoring of sensitive cargo, such as railway fuels |
| **ESF #2 – Communications** | Yolo Emergency Communications Agency | • Conduct emergency communications and public alert & warning as early as possible.<br>• Provide status of all primary and alternate communications affected by, or affecting response to, cyber incidents<br>• Provide alternate communications during potential cyber incidents impacting GIS and digital communications |
| **ESF #5 – Emergency Management** | Yolo County Office of Emergency Services | • Activate EOC as needed based upon EOP<br>• Provide over-arching ESF coordination with the Regional Emergency Operations Centers (REOCs)/SOC, Joint Field Office (JFO), Regional Fusion Centers (RFC), and other emergency functions<br>• Coordinate during cyber incidents impacting GIS, the Web Emergency Operations Center (“WebEOC”) system, and other forms of response technology<br>• Coordinate the collection of status information for all technology-based systems, devices, and connections affected by, or affecting the response to, a cyber incident<br>• Provide state and local leadership with current status of all technology-based systems, devices, and connections |

| | | |
|---|---|---|
| | | consistently throughout a cyber incident<br>• Affected Department PIO is notified and activates countywide joint information systemin coordination |
| **ESF #7 – Logistics & Resource Management** | Yolo County General Services | • Provide alternate data processing sites and incident reporting to facilitate and support successful data processing from an alternate location during a cyber-event<br>• Coordinate during cyber incidents impacting industrial control systems |
| **ESF #8 – Public Health & Medical** | Yolo County Department of Health Services | • Assess potential impacts to residential care facilities<br>• Coordinate during cyber incidents impacting public health and medical functions including, but not limited to, emergency management, healthcare facility durable equipment/infrastructure, food/drug, and radiological/nuclear systems |
| **ESF #10 – Oil & Hazardous Materials** | Yolo County Environmental Health Division and Operational Area Fire Coordinator | • Coordinate during cyber incidents impacting the equipment that monitors and releases hazardous materials, controlled by industrial control systems |
| **ESF #11- Agriculture and Natural Resources** | Yolo County Agricultural Commissioner | • Coordinate during cyber incidents impacting manufacturing equipment and other industrial control systems used in Food and Agriculture |
| **ESF #12 – Energy** | Pacific Gas & Electric | • Coordinate during cyber incidents impacting industrial control systems that support critical infrastructure |
| **ESF #15 – External Affairs** | County Administrator or designee<br>Public Information Officer (PIO) | • Coordinate public information with impacted local jurisdictions<br>• Coordinate the content and release of security notifications to the public and receiving information from Public Information Officers |

## 2.3 Regional Assistance

Successful operation of the Yolo County cyber security annex requires coordination with a diverse group of stakeholders, including regional partners. Regional Fusion Centers (RFCs) in particular, play a key role in cyber incident response at the regional level. Fusion centers provide valuable intelligence and response capabilities that can contribute to the mission of this annex.

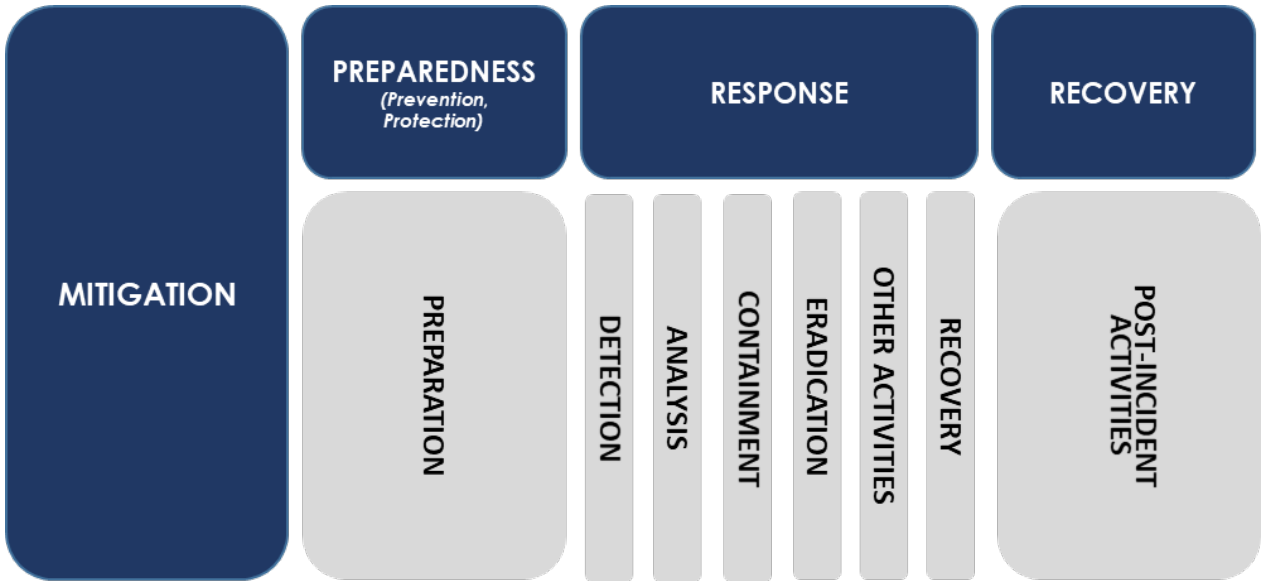
A primary responsibility for RFCs is to provide situational awareness on incidents to the Chief Information Security Officer (CISO). These fusion centers can provide situational awareness updates to CISO even when they are not requesting support from state entities. This one-way communication allows CISO to remain aware of ongoing threats and provide expeditious support when requested. Fusion centers may also request state-level incident response support from CISO, including support for information and resource sharing. When support is requested, CISO can leverage state resources as well as connect regional entities to other actors with a given set of specialized skills or resources.

# Section 3.0: Concept of Operations

## 3.1 Cyber Incident Management Phase

Cyber incidents require the involvement of both information technology experts and emergency management. To provide clarity to all sides of the multi-faceted response partners, the following matrix (Table 4) depicts the overlap between emergency management activities and information technology activities, using terminology familiar to each set of stakeholders.

**Table 4: Cyber Incident Management Process in Relation to Emergency Management Phases**



## 3.2 INCIDENT RESPONSE TEAMS

Incident Response Teams (IRT) will be established and facilitated by the Yolo County Innovation and Technology Services to lead the cyber response efforts. During the initial conference between the affected entity, the Chief Information Security Officer will activate the teams of pre-appointed team members. The teams will communicate and work together with staff, local, state, and federal resources to identify the threat, develop threat intelligence, and analyze actual or potentially affected systems, and work to remediate the incident. The amount of IRTs responding to an incident will depend if the incident is affecting a single department, multiple departments, the County, or entities outside the County itself.

The Incident Response Teams will notify and coordinate with YCOES for SEVERE and EMERGENCY cybersecurity incidents. If warranted, YCOES will activate elements of the County's Emergency Operation Plan (EOP). This could result in the activation of the EOC to facilitate information sharing, resource development, and operational coordination.

Upon activation, the IRTs will be responsible for:

- Implementing tactical response operations to detect, analyze, contain, eradicate, and recover from an incident within their respective line(s) of effort
- Receiving strategic direction and guidance from governing authorities and aligning response actions appropriately
- Coordinating with public and private sector entities within the state to implement proper threat detection, reporting, and response procedures
- Establishing a regular reporting schedule to provide updates to governing authorities to create and maintain situational awareness and support operational coordination and coordinating with Emergency Operations Command to:
    - Conduct briefings or share information with non-state partners
    - Provide recurring reporting to Federal entities using designated reporting procedures to meet regulatory requirements, and create and maintain situational awareness at the federal level
- Providing support to law enforcement agencies responsible for criminal investigation and reporting during cyber incidents and state agencies responsible for advancing information security.
- Facilitating the collection and proper handling of evidence
- Providing technical support to the affected entity to facilitate cyber incident resolution

## 3.3 CYBER INCIDENT RESPONSE LINES OF EFFORT

As described in Table 5 below, there are four lines of effort in cyber incident response: Threat Response, Asset Response, Intelligence Support, and Affected Entity Response. These concurrent lines of effort provide the foundation required to synchronize various response efforts before, during, and after a cyber incident, as defined below.

**TABLE 5: Cyber Incident Response Lines of Effort, Defined**

| Line of Effort | Definition |
|---|---|
| **Threat Response** | Activities include the appropriate law enforcement investigative activities for:<br>· Collecting evidence and gathering intelligence to provide attribution<br>· Linking related incidents and identifying additional possible affected entities<br>· Identifying threat pursuit and disruption opportunities<br>· Developing and executing courses of action to mitigate the immediate threat and facilitating information sharing and coordination with Asset Response efforts |
| **Asset Response** | Activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents by:<br>· Identifying other entities possibly at risk and assessing their risk to the same or similar vulnerabilities<br>· Assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks<br>· Facilitating information sharing and operational coordination with Threat Response<br>· Providing guidance on how best to utilize state and local resources and capabilities in a timely, effective manner to speed recovery |
| **Intelligence Support** | Facilitates the building of situational threat awareness and sharing of related intelligence to:<br>· Create an integrated analysis of threat trends and events<br>· Identify and assist with the mitigation of knowledge gaps<br>· Suggest methods to degrade or mitigate adversary threat capabilities |
| **Affected Entity Response** | · Highly encouraged to share information surrounding the event with other cybersecurity specialists to assist with the investigative, analysis, response, and recovery phases of cyber incident response<br>· The affected entity is the data owner and retains responsibilities to ensure appropriate actions and safeguards are in place to remediate threats and secure their information |

## 3.4 AFTER-ACTION REVIEW

The purpose of after-action reporting is to provide a mechanism where shortfalls and limiting factors can be captured and documented. They can then be improved on as part of an ongoing improvement effort. OES and responding departments are responsible for compiling and developing the After-Action Report (AAR). Individuals assigned to the event will assist in the effort by providing input and attending debriefing sessions. All After Action Reports are due within 90 days of the end of the event.

# APPENDIX A: TEMPLATE- DEPARTMENT NAME COOP

The purpose of this appendix is to link your department continuity of operations plan (COOP) to Yolo County's Cyber Security Annex. Your COOP describes the steps department personnel will take if there is a disruption in normal operations. The cyber security annex identifies the steps each department's information technology staff will take if the disruption is cyber-related. It also describes how the information technology team will work with the department preparedness coordinator to jointly respond to the incident, continue department operations, reconstitute essential systems and return to normal operations.

Begin by identifying the essential functions your department is responsible for.

| Essential Function | | Supporting IT Systems |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |

An event has three phases: before (pre), response (during) and recovery (after). Answer the following questions to document the resources available, individuals that need to be notified and steps the IT team and YCOES will take relating to a cyber event.

| Pre-event | Department Response |
|---|---|
| 1. What are the tools and techniques used to analyze system security? | *List of Tools:*<br>*List techniques:*<br>*Which group/team is involved in performing analysis in your department?* |
| 2. How will you ensure that your Department are available to support County and ITS cyber incident response and recovery process? | *Who in your department will own this responsibility?* |
| **During an event** | **Department Response** |

| | |
|---|---|
| 3. What are the tools and techniques used to analyze a cyber incident? | *List of Tools:*<br>*List techniques:*<br>*Which group/team is involved in performing analysis in your department?* |
| 4. How and when will the Yolo County Innovation and Technology Services (YCITS) get notified of an incident? | *Who will notify ITS?*<br>*Do you have your ITS contact information stored?* |
| 5. How would this issue be reported in your Department leadership? | *Email? Phone Call? Everbridge?* |
| 6. Classify your department critical IT applications/systems based on ESF priority Matrix | *Collect this information and Add this information on COOP* |
| 7. What priority will be assigned based on ESF 18 Matrix? | *How and who will determine the priority* |
| 8. What is the process and who will be involved to participate in emergency response? | *Who owns the process? Is training provided to your dept on emergency response process?* |
| 9. How are communications handled internally to department staff and senior management? | *Phone? Email? Everbridge? Social Media?* |
| 10. What's the department guidelines on media relations? | *Collect this information from your department PIO or Communications Team* |
| 11. Who is designated to talk to the press? | *Collect this information from your department PIO or Communications Team* |
| **After an event** | **Department Response** |
| 12. Who in the Department will request and approve emergency procurement for laptops or server equipment? | *Collect this information from your Department Finance* |
| 13. As restoration may take several months, have you determined alternate/back up procedures to continue your Department operations without internet and computers in your Department COOP? | *Collect this information from your Department Management* |
| 14. How are you tracking costs of getting your system back online? | *Collect this information from your Department Finance* |

# APPENDIX B: VERSION HISTORY

| Change Number | Section | Date of Change | Individual Making Change | Description of Change |
|---|---|---|---|---|
| | All | 5/26/2024 | Yolo OES | Revised |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# APPENDIX C: GLOSSARY

- **Cyber Attack-** Criminal activity conducted using computers and the Internet. This includes a broad range of activity from downloading illegal music files to monetary theft, fraud, distributing malware, posting confidential information, and identity theft.
- **Cyber Crime-** Criminal activity conducted using computers and the Internet. This includes a broad range of activity from downloading illegal music files to monetary theft, fraud, distributing malware, posting confidential information, and identity theft
- **Cyber Incident-** An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or data. A cyber incident may impact organizational operations (including mission, capabilities, or reputation). A significant cyber incident is an incident (or group of related incidents) that is likely to result in demonstrable harm to public health and safety, critical functions, civil liberties, economy and/or community.
- **Cyber Security-** The process of protecting information and systems by preventing, detecting, and responding to threats and attacks.
- **Data Breach**- A data breach is the release of nonpublic information to an untrusted entity. Nonpublic data Includes but not limited to: Medical (HIPAA), Financial (PCI/Nacha), Identity (PII), Legal/law enforcement data
- **Emergency Support Function (ESF)** – A functional area of response activity established to facilitate the delivery of Federal assistance required during the immediate response phase of a disaster to save lives, protect property and public health, and to maintain public safety. ESF represent those types of federal assistance that the State would most likely need because of the overwhelming impact of a catastrophic or significant disaster on its own resources and response capabilities or because of the specialized or unique nature of the assistance required. ESF missions are designated to supplement state and local response efforts.
- **Event-** Any observable occurrence in a network or system. False Positive: An alert that incorrectly indicates that malicious activity is occurring
- **Exploit-** A piece of software or sequence of commands that take advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software or hardware. A Zero Day Exploit is a new, previously unknown vulnerability
- **Fusion Center** - Fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal and state, local, tribal, territorial and private sector partners

- **Support Agencies** - Support agencies provide resources and staffing that contribute to the overall accomplishment of the mission of the County's Support Function. Not every Support Agency will have input to, or responsibilities for, the accomplishment of every mission assigned to the County's Support Function.
- **Threat**- Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For cyber threats this also includes the potential source of an adverse incident.