

SACRAMENTO COUNTY

OFFICE OF EMERGENCY SERVICES



CYBER HAZARD ANNEX



December 2022

HANDLING INSTRUCTIONS

1. The title of this document is the *Sacramento County Cyber Hazard Annex*.
2. The information gathered herein is to be used for training and reference purposes within Sacramento County. Reproduction of this document, in whole or in part, without prior approval from the Sacramento County Office of Emergency Services is prohibited.
3. The Cyber Hazard Annex is available at www.sacoes.org. Alternative formats (e.g., Large Print) can be made upon request with the point of contact below.
4. Point of Contact:

Matthew Hawkins
Emergency Operations Coordinator
Sacramento County Office of Emergency Services
hawkinsm@sacoes.org
(916) 874-4670 office

RECORD OF CHANGES

(Note: File each revision transmittal letter behind this record page.)

REVISION NUMBER	ENTERED BY	PURPOSE	PAGE NUMBER	DATE
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

TABLE OF CONTENTS

HANDLING INSTRUCTIONS.....	i
RECORD OF CHANGES	ii
TABLE OF CONTENTS	iii
1.0 INTRODUCTION.....	1
1.2 Scope	3
1.1 Situation	4
1.2 Planning Assumptions.....	4
1.3 Authority and References	5
1.4 Plan Maintenance	6
1.5 Training and Exercises.....	7
2.0 CONCEPT OF OPERATIONS.....	8
2.1 Overview	8
2.2 Incident Classification Levels	9
2.3 Plan Activation and Notifications.....	10
2.4 EOC Structure for a Cyber Incident.....	12
2.5 Organizational Roles and Responsibilities	14
2.6 Public Information Release	18
3.0 INCIDENT RESPONSE	19
3.1 Process Overview	19
3.2 Step 1: Preparation	20
3.3 Preparation Phase Responsibilities and Actions	20
3.4 Step 2: Detection and Analysis.....	21
3.5 Detection and Analysis Phase Responsibilities and Actions	22
3.6 Additional Responsibilities and Actions Required for Severe Cyber Incidents.....	23
3.7 Step 3: Containment, Eradication and Recovery	24
3.8 Containment and Eradication Phase Responsibilities and Actions.....	25
3.9 Recovery Phase Responsibilities and Actions	26
3.10 Step 4: Post Incident Review.....	27
4.0 CRITICAL CONSIDERATIONS	29

Sacramento County
Cyber Hazard Annex

4.1	Critical Considerations	29
4.2	Preparation	29
4.3	Detection and Analysis Phase	30
4.4	Containment, Eradication, and Recovery Phase	32
	Appendix A – Acronyms	34
	Appendix B – EOC Cyber Incident Checklist.....	36
	Appendix C – EOC Cyber Incident Essential Elements of Information.....	38
	Appendix D – Cyber Incident Notification Form	40
	Appendix E – Contact List Government Response Organizations.....	42
	Appendix F – Vendors	43
	Appendix G – CITF Points of Alternative Contact Means.....	44
	Appendix H – IT System Outage Scorecard.....	45
	Appendix I – Major Cyber Threat Actors and Attack Methods.....	46

1.0 INTRODUCTION

Cyber Incidents interfere with or degrade mission-critical technology, which impairs the ability of organizations to conduct normal operations. In some cases, life-health and safety impacts can be caused. The ability of Sacramento County to maintain the continuity of its operations, react to various situations, and deliver services to its community can all be impacted by a Cyber Incident.

The Sacramento County Cyber Hazard Annex supports the Sacramento County Emergency Operations Plan (EOP). This Annex outlines Sacramento County's response activities, including the Emergency Operations Center (EOC) response processes, for a Cyber Incident that impacts the County's Information Technology (IT) Systems, networks, infrastructure and/or data. It is the intent of this Annex to create a framework for preparations and response within existing statutory obligations and limitations based on state and/or federal guidance for cyber-attacks.

This Annex does not apply to smaller events that may cause minor disruptions to County IT Systems and their operations, but rather, it focuses on circumstances where a significant impact to one or more of the County's IT Systems occurs and requires a coordinated inter-agency response to support actions taken by the Department of Technology (DTech) and the Chief Information Security Officer (CISO) per the DTech Security Incident Response Plan (SIRP).

The following are key terms and concepts used in this plan:

Cyber Incident: Any "Security Incident" as defined in the SIRP that has or may have an adverse operational impact on the confidentiality, integrity, or availability of County IT Systems and the data they store, process, or transmit.

"HIGH" Cyber Incidents: A limited attack resulting in moderate to significant consequences that are occurring or are imminent, including security related County service disruptions with limited impacts on County operations.

IT Systems: As defined in the SIRP, these are the combination of computing devices (e.g., laptops, desktops), IT infrastructure (e.g., servers, network equipment), and software that deliver technology solutions to enable the operation of Sacramento County Departments and Agencies, including, but not limited, to "County IT resources".

“SEVERE” Cyber Incidents: An attack resulting in highly disruptive consequences that are occurring or are imminent, including security related County service disruptions with significant impacts on County operations.

Critical Infrastructure: The systems and assets, whether physical or virtual, so vital to Sacramento County that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, economic security, public health or safety, or any combination of those matters.

Sacramento County Department of Technology (DTech): The central information technology and telecommunications service provider for Sacramento County employees, departments, and regional partners responsible for the County’s IT Systems and Infrastructure.

Government Response Organizations: Those federal and state organizations, and others aligned with them, that have significant interest and equities associated with Cyber Incident response and that may provide support to Sacramento County.

IT Systems: These are the combination of computing devices, (e.g., laptops, desktops), IT infrastructure (e.g., servers, network equipment), and software that deliver technology solutions to enable the operation of Sacramento County Departments and Agencies, including, but not limited, to “County IT resources.”

Security Incident Response Plan (SIRP): The Sacramento County Department of Technology Security Incident Response Plan adopted October 2021, as amended.

1.1 Purpose

The purpose of this Cyber Hazard Annex is to define the operational concepts and responsibilities of various stakeholders during a Cyber Incident affecting Sacramento County Department and Agency IT Systems, and which require a response coordinated by the EOC. It is comprised of procedures to identify, coordinate, remediate, recover, and track successful mitigations from Cyber Incidents and vulnerabilities affecting County IT Systems. This includes the following:

- Provide a system to evaluate the severity of a Cyber Incident and appropriate EOC response levels.
- Define the role of the EOC and County departments in a Cyber Incident declared by the CISO.

- Assign roles and responsibilities to County stakeholders to support a response to a Cyber Incident.
- Establish a common understanding of key cyber concepts and terminologies.
- Provide guidance to manage the disruption, impairment or interruption of IT Systems relied upon by Sacramento County Departments and Agencies to perform their missions.

1.2 Scope

This Annex is focused on response activities required when **HIGH** and **SEVERE** Cyber Incidents impact County operations resulting in the activation of the County EOC. While it may be useful, this Annex is not intended to guide the response to lower-level security incidents or events (classified in the SIRP as **ELEVATED** or **GUARDED**) or the mere loss of sensitive information, all of which are otherwise addressed in the SIRP.

This Annex applies to all Sacramento County Departments and Agencies that rely on DTech for their IT Systems, except the County Sheriff's Office, District Attorney, and Superior Court who manage their own IT Systems and are not governed by this Annex, though they may participate in Annex-related response activities at their discretion. The Sacramento County Department of Airports is principally supported by DTech for their IT Systems, though some are separately managed. The Department of Airports will participate in response activities and is considered in scope for application of this Annex.

During **HIGH** Cyber Incidents, the EOC will primary be focused on maintaining a shared operational picture and situational awareness in support of the DTech Security Incident Response Team (SIRT) activities. In cases of **SEVERE** Cyber Incidents, the County's EOC is activated to:

- Develop and maintain a common source of situational awareness of the impacts of the disruption on County Departments and Agencies.
- Coordinate Department and Agency operational response in a cyber-disrupted environment.
- Manage the sourcing and provision of resources needed by DTech and Sacramento County Departments and Agencies in responding to the Cyber Incident.
- Coordinate internal and external communications regarding impacts to County services and operations.
- Establish key processes for sharing information available to support Cyber Incident response activities and to enhance the awareness and capabilities of external organizations.

1.1 Situation

This Annex is focused on two major concurrent operational efforts:

1. Coordination of, and support to, county-wide operational responses by its Departments and Agencies to mitigate the disruptions caused by **HIGH** and **SEVERE** Cyber Incidents to their IT Systems; and
2. Supporting DTech as it executes its responsibilities under the SIRP to respond to **HIGH** and **SEVERE** the Cyber Incidents, including but not limited to; managing external communications, Government Response Organizations inquires and overarching response activities, executive-level communication and traditional EOC activities such as logistics and procurement of equipment and services.

1.2 Planning Assumptions

Certain assumptions were used during the development of this Annex. These assumptions include basic principles related to cyber threats and their impacts on the community.

- A **SEVERE** Cyber Incident will require a complex, whole-of-county response to mitigate community impacts from the disruption of County operations and will pose challenges in terms of resources, Department and Agency coordination, information sharing, and logistics.
- Significant disruptions to County Departments and Agencies associated with Cyber Incidents are most likely to occur during the *Detection and Analysis* phase of incident response.
- A Cyber Incident can impact traditional communication systems (such as email), and therefore alternative channels of communication may be needed throughout the duration of the incident.
- A Cyber Incident may be of indeterminate impact and uncertain duration. Accordingly, the execution of County and Department Continuity of Operations Plans (COOP) plans may be delayed or deferred as the Cyber Incident response activities are performed by DTech. This Annex is intended to guide and coordinate County Department and business unit response activities prior to any execution of their individual COOP plans and thereafter through the Cyber Incident Task Force (CITF, discussed herein) once it is activated by the EOC. In some cases, Departments and Agencies

may elect to mitigate the impacts of even a Severe Cyber Incident without execution of their COOP plan.

- Government Response Organizations may actively seek to engage DTech during its response activities to gather information and to provide support. This Annex assumes that during **SEVERE** Cyber Incidents, the EOC will serve as the point of coordination on behalf of DTech for these purposes.
- Critical information is frequently difficult to gather in Cyber Incidents, including the scope of impacts, the time to recover systems, and even whether the Cyber Incident is under control. Communicating these facts together with the impacts of a Cyber Incident to the citizens and stakeholders in Sacramento County requires a carefully orchestrated public communication strategy. The collection of relevant and timely information is critical to unambiguous communications and dissemination of accurate updates and guidance to the public.

1.3 Authority and References

This Annex interacts with other relevant documents, guidance, and plans. This Annex is not intended to replace existing documentation, but rather supplement it. This Annex was developed to complement the SIRP, the County EOP, is aligned to the guidance established under NIST SP 800-61, and the Annex to the California State Emergency Plan for ESF #18 for Cyber Security.

A detailed list of authorities and references related to the emergency operations process are provided in the Sacramento County *Emergency Operations Plan, Section 1: Plan Administration*. Authoritative documents specific to a Cyber Incident are outlined in Table 1 below.

Table 1: Cyber Incident Authorities

Authorities	
Local	
Department of Technology Continuity of Operations Plan, County of Sacramento, March 2021	This DTech COOP Plan is an annex to the Sacramento County COOP Plan and supports DTech in preparing for and responding to COOP-related emergencies and supports operations and decision-making for continuity of the department’s essential functions following an emergency event.
Department of Technology Security Incident Response Plan, County of Sacramento,	This document describes the overall plan for responding to County of Sacramento Wide Area Network (CoSWAN) security incidents.

October 2021 (aka: SIRP)	
Emergency Operations Plan, County of Sacramento, as amended (aka: EOP)	The Sacramento County Emergency Operations Plan (EOP) establishes an Emergency Management Organization and assigns functions and tasks consistent with California’s Standardized Emergency Management System (SEMS) and the National Incident Management System (NIMS). It provides for the integration and coordination of planning efforts of multiple jurisdictions within Sacramento County.
Sacramento Countywide Local Hazard Mitigation Plan Update, County of Sacramento September 2021	The purpose of hazard mitigation is to reduce or eliminate long-term risk to people and their property from hazards. Sacramento County developed the Local Hazard Mitigation plan (LHMP) update to make the County and its residents less vulnerable to future hazard events.
State	
California Government Code Section 8558 (2018)	Senate Bill 532 amended Section 8558 of the Government Code to include cyberterrorism in the conditions that constitute a state of emergency and local emergency.
California Government Code Section 8586.5 (2018)	Assembly Bill 2813 added section 8586.5 to the California Government Code, which codified Cal-CSIC in state law. Cal-CSIC was originally the result of Executive Order B-34-15.
Federal	
National Institute of Standards and Technology (NIST) 800-53 (2013) and 800-61(2008)	NIST Special Publications 800-53 and 800-61 provide recommendations and guidance for federal-level cyber incident management. 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, provides a menu of recommended controls for protecting organizational operations and assets against cyber threats. 800-61, the Computer Security Incident Handling Guide, provides operations response guidance for computer security incidents, including information on building response capabilities, analyzing incident data, and determining the level of response required by an incident.

1.4 Plan Maintenance

The Sacramento County Office of Emergency Services (Sac County OES) has the primary responsibility for ensuring that necessary changes and revisions to this plan are prepared, coordinated, published, and distributed. Changes to the SIRP and COOP plans should be carefully coordinated with this Annex to ensure continuing alignment. This Annex will be reviewed annually, with a full document update

conducted not less than biennially and after development of significant lessons learned around its implementation.

Elements of this Annex may also be modified by Sac County OES any time due to changes in state and/or federal mandates, operational requirements, or statutes so require. Once distributed, new editions to this Annex shall supplant older versions and render them inoperable.

1.5 Training and Exercises

Elements in this Annex should be incorporated in the County's training and exercise program to ensure users are familiar with the concepts and that they receive adequate training on the processes, procedures, and roles and responsibilities contained within it.

2.0 CONCEPT OF OPERATIONS

2.1 Overview

This Annex will be used for those Cyber Incidents that are designated **HIGH** or **SEVERE**. The SIRP provides detailed processes for response activities to be performed by DTech for a range of events and incidents. This Annex will be used for those Cyber Incidents that are designated **HIGH** or **SEVERE**. While some coordination activities with the County's Departments and Agencies are discussed in the SIRP, in the most severe cases, effective coordination of County Departments and Agencies during **HIGH** or **SEVERE incidents** is outside the scope of the SIRP. Use of this Annex allows for the utilization of the County's EOP, including the activation of the EOC to manage the coordination efforts of a cyber response, allowing for DTech to focus on its response to the Cyber Incident and ultimately restoration of services.

When activated, the EOC's actions will support and be consistent with the NIST 4-Step Security Incident Response Cycle process which will be used by DTech to resolve the Cyber Incident.

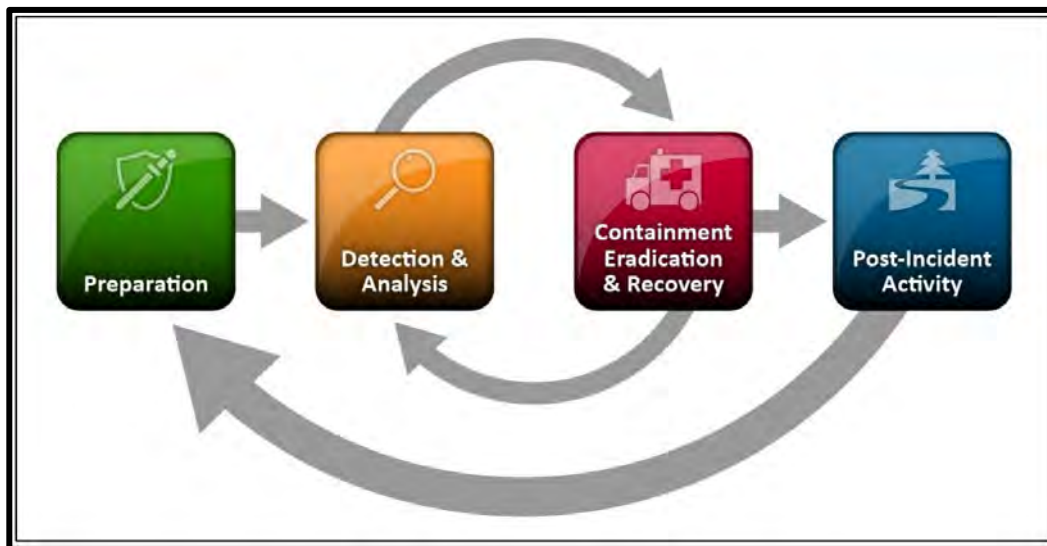


Figure 1. NIST Security Incident Response Life Cycle

Cyber Incidents are a regular occurrence and the SIRP provides for an escalating set of responses for DTech, which generally begin with detection and then are supported by analysis. In most cases, the Cyber Incident is detected by security technology or human reporting and is rapidly mitigated through manual or automated containment, eradication, and recovery actions. In such cases, IT

System users are frequently unaware of the onset or completion of the response life cycle shown above. This Annex is not invoked in such common cases, usually designated **GUARDED** or **ELEVATED**, and which are managed exclusively under the SIRP or normal DTech operational processes.

2.2 Incident Classification Levels

The following chart is a method for rating the current or potential priority of a cyber incident upon County Departments and Agencies, as defined in the SIRP. During **ELEVATED** or **GUARDED** level incidents, this Annex is not intended for use in coordinating response activities by DTech or Departments and Agencies, which should generally be governed by the SIRP. However, for such incidents, DTech may notify the EOC duty officer for situational awareness, but such notifications to the EOC are not required, and the EOC need not take any action. Figure 2 below describes the Cyber Incident classification schema and summarizes key elements of response activities related to Notifications and EOC Activation.

Cyber Incident Classification Levels			
	Action Required	Description	Disruption Characteristics
SEVERE	Notification to EOC Notification to Leadership CISO Notification to Cal-SCIC and FBI EOC Activation in Support of Declared Cyber Incident by CISO Activation of the CITF	<p>Attack</p> <p>Highly disruptive consequences are occurring or imminent.</p>	<ul style="list-style-type: none"> • Security related service disruption with significant impact on County operations. • An incapacitated municipality or critical infrastructure • Significant loss of confidential data. • Loss of mission-critical systems or applications. • Significant risk of negative financial or public relations impact resulting from a security issue. • An effective attack that is difficult to control or counteract. • > 1 hour outage Public Safety Health Services, Human Assistance, phone systems, internet, 9-11, public address system, EOC, building 600 (> 5 min active) resulting from a security issue. • >6 hour outage any other system resulting from security issue.
HIGH	Notification to EOC EOC to monitor the Event	<p>Limited Attack(s)</p> <p>Moderate to significant consequences are occurring or imminent.</p>	<ul style="list-style-type: none"> • Security related service disruption with limited impact on County operations. • Small number of systems compromised. • Little or no loss of confidential data resulting from security issue. • Small risk of negative financial or public relations impact resulting from security issue. • Minimally successful attack is easy to control or counteract. • Widespread instances of a new computer virus or worm that cannot be handled by deployed anti-virus software. • Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software. • >1 hour outage of any major system resulting from security issue.

Cyber Incident Classification Levels				
	Action Required		Description	Disruption Characteristics
ELEVATED	Notify CISO No notification to EOC required	Handled at the Department/DOC Level	<p>Risk of Attack</p> <p>Early indications of moderate to severe consequences</p>	<ul style="list-style-type: none"> • A significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance. • Penetration or denial of service attack(s) attempted with minimal impact to County of Sacramento operations. • Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software. • Intelligence received concerning threat to which County systems may be vulnerable. • >30 minute < 1 hour any major system resulting from a security issue.
GUARDED			<p>Baseline Risk of an Attack</p> <p>Unlikely to impact public health or safety, or city services.</p>	<ul style="list-style-type: none"> • Initial report of a cyber event. • Malware or malicious content that has a low probability of spreading, such as malware detected by an anti-virus on a workstation • Small numbers of system probes, scans and similar activities detected on external systems. • Isolated instances of known computer viruses or worms, easily handled by deployed anti-virus software. • < 30 minute major system resulting from a security issue.

Figure 2: Cyber Incident Classification Levels

2.3 Plan Activation and Notifications

As the Incident Commander (IC), the CISO is empowered to both activate this Annex and notify the EOC to request its activation in response to a Cyber Incident. This Annex is triggered/activated when a Cyber Incident is classified by the CISO as **HIGH** or **SEVERE** resulting in the CISO, or the CISO’s designee, notifying the EOC Duty Officer of the incident. Activation of the Annex will result in activation of the EOC as outlined in section 2.4.

If at any point the incident level changes (i.e.: escalates from **GUARDED** to **HIGH**, or **HIGH** to **SEVERE**) additional action steps should be taken for the appropriate level of EOC activation to support the evolving incident.

The primary means by which the CISO, or the CISO’s designee, will notify the EOC is through the SacAlert notification system. If, due to the incident, the SacAlert system is not functioning, the CISO may use email, Skype for Business, phone, in-person, or any other available secure means to notify the EOC.

Activation Steps:

(Note: the chart below uses arrows to indicate notification requirements, and bubbles to indicate action items)


The determination of the incident level of event is determined at the discretion of the CISO. Upon determination of a Cyber Incident, the CISO will assume the role of Incident Commander and begin following the SIRP process.

Upon the initial report or detection of a Cyber Incident, the following steps will be followed by the DTech team:

- 1 Conduct initial incident impact analysis
- 2 Identify IT system affected
- 3 Determine the appropriate level of event (**GUARDED/ELEVATED/HIGH/SEVERE**)

If the incident is **GUARDED** or **ELEVATED**, no notification to the EOC is required. In this case, the Cyber Incident will be handled at the department level by DTech.

If the Incident is declared **HIGH** by the CISO, the response will require an involvement of the EOC and an activation to begin monitoring the situation. Upon declaration of a **HIGH** -level incident, in addition to the required steps above, DTech will:

- 1 Assume the role of Incident Commander
- 2 Activate the DOC to support response
- 3 Activate the SIRT
- 4  The CISO will notify the Sac County OES Duty Officer and request EOC Activation
- 5 The EOC will activate to a Level 4 (Duty Officer/Monitoring Level) to monitor the situation. Based on EOC discretion, the EOC may choose to activate at a higher level (Levels 3, 2 or 1) - if determined necessary.

If the Cyber incident is declared or expands to a **SEVERE**-level event, the CISO will continue to serve as the Incident Commander and oversee the IT response and will additionally notify the Sac County OES to activate the EOC to

coordinate and support overall response activities. Once DTech determines the event to be **SEVERE**, the following response process will be used:

- 1 CISO to notify the OES Duty Officer and request EOC Activation
- 2 EOC to activate a Level 1 or 2 to begin coordinating the response and initiate the Cyber Hazard Annex
- 3 Send appropriate level of DTech representative to EOC to staff Branch
- 4 CISO (or the EOC if requested by the CISO) will notify appropriate Government Response Organizations of the confirmation of a Cyber Incident
- 5 EOC to notify relevant city leadership, and supporting ESF Departments and Agencies
- 6 EOC activates CITF and coordinates response activities with relevant County Departments and Agencies
- 7 EOC will assess County Department and Agency needs and coordinate necessary resources
- 8 EOC will coordinate release of public information with impacted departments, and/or the joint information center (JIC), if activated
- 9 EOC will coordinate incoming and outgoing support/resource requestions with relevant local/state/federal entities
- 10 SIRT will provide and receive sit stat reports to/from the EOC and prepare for formal EOC briefings

The EOC will continue to repeat steps 7 – 10 until the Cyber Incident is resolved. The CISO and SIRT should ensure that information continually flows between the DTech DOC/SIRT and the EOC to frequently assess resource needs and develop, and adjust, an appropriate public information strategy, and to keep Sacramento County leadership informed. Upon resolution of the cyber event, both the DOC and the EOC will be deactivated.

2.4 EOC Structure for a Cyber Incident

For a Cyber Incident, the EOC may activate at any of its current levels – one, two, three or four – depending on the scope and scale of the Cyber Incident.

The four levels of activation provide varying EOC staffing commensurate with the coordination needs of emergency situations. The goal is a rapid EOC activation when it is needed. During an active incident, the EOC will have a supporting role and act as a resource available to the Cyber IC, as needed. The EOC is at the disposal of the IC and will interface with outside agencies as set out in this Annex.

During a **HIGH-level** Cyber Incident, the EOC will normally undertake a partial activation, such as a level two or three. In a **HIGH-level** Cyber Incident, the EOC will begin to gather relevant information, ensure that internal notifications are made, and provide support to DTech as requested.

When fully activated, as outlined in Figure 3 below, in support of a **SEVERE-level** Cyber Incident, the EOC will be organized to incorporate the functions, roles, and expertise needed, including incorporating the CITF. The CITF is managed by the EOC Director's designee. When the DTech DOC is functioning either autonomously or concurrently with the EOC, the CISO will serve as the Cyber Incident Commander/DTech DOC Director.

The coordination among the EOC Sections is managed in accordance with the guidance and processes described in the County EOP. Each EOC Section will activate any branch or unit necessary to support the response.

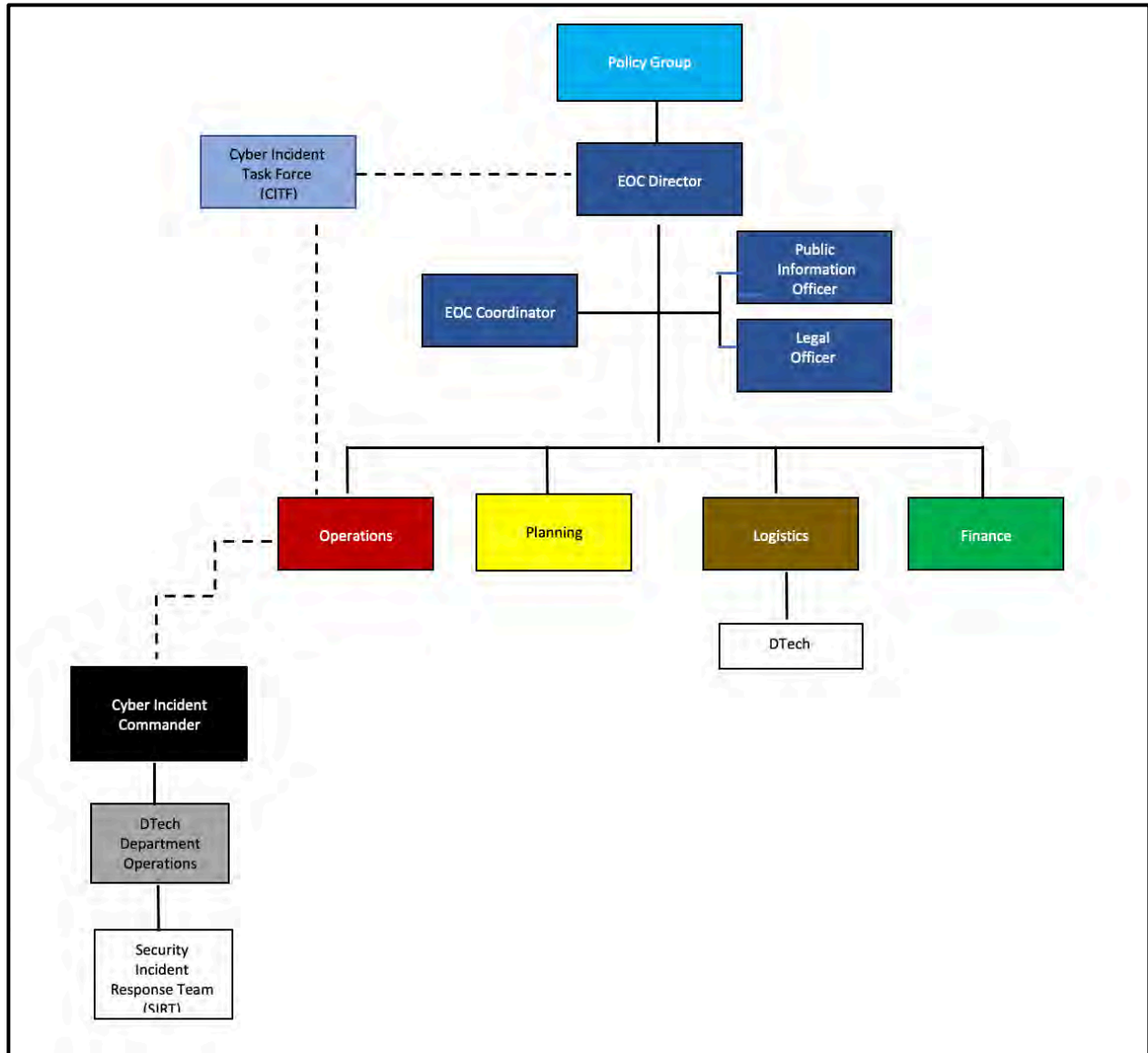


Figure 3. Level 1 EOC Activation for a SEVERE Cyber Incident

2.5 Organizational Roles and Responsibilities

During a **HIGH** or **SEVERE** Cyber Incident, DTech leads the response and Sac County OES supports DTech through the EOC. In the case of a **SEVERE** Cyber Incident, the CITF will be activated by the EOC to provide the coordination body for mitigating operational impacts to County services and operations. The following agencies will have a **primary role** in responding to a Cyber Incident:

Department of Technology (DTech): The designated DTech official responsible for the overall organizational cyber security posture and serves as the lead County authority in responding to cyber security incidents. During the response phase,

DTech will have the primary responsibility for implementing tactical cyber response activities.

The DTech is led by the Chief Information Officer (CIO) who is responsible for Sacramento County's strategic use of technology, managing the Department of Technology, and working closely with County Departments and Agencies to implement IT systems that improve business processes and enhance citizen services. The CIO reviews the acquisition of IT services, systems, and resources for consistency with established standards, and works with the County Executive's Office to secure funding for IT projects. **The CIO also serves as the County Chief Information Security Officer (CISO).**

Sacramento County Office Of Emergency Services: (Sac County OES): Has the responsibility for coordinating responses to all emergency events impacting Sacramento County and manages the EOC. During a declared HIGH or SEVERE Cyber Incident, Sac County OES will support the Cyber Incident Commander, as set out in this Annex.

County Departments and Agencies will have secondary supporting responsibilities to the lead agencies in Cyber Incident response. These Departments and Agencies may include any directly supporting the response, those with business operations and/or services that may be impacted, and those that have cross-cutting interactions with other ESF's (e.g., Social Services, Transportation, Communication).

Cyber Incident Task Force (CITF): The CITF will be convened by the EOC Director for a **SEVERE** Cyber Incident to provide expertise regarding the operational (i.e., non-IT) impacts upon individual County business services and operations. The CITF will serve as a Multiagency Coordination Group consistent with the Sacramento County EOP. The CITF is comprised of representatives from the County Departments and Agencies that can speak authoritatively on the business and service impacts of the incident and the steps being taken by their respective Departments and Agencies to address those impacts. When activated, the CITF will serve as the information sharing conduit between County Departments and Agencies and the EOC, provide coordinated decision-making and resource allocation among County Departments and Agencies, and may establish business impact priorities, harmonize business impact policies, and provide strategic guidance and direction to support incident management activities.

Government Response Organizations: Other external supporting governmental and law enforcement agencies will support DTech and the County of Sacramento to resolve a Cyber Incident. These Government Response Organizations include the Central California Intelligence Center (CCIC), the DHS Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of

Investigation (FBI), and the California Cyber Security Integration Center (Cal-SCIC). These agencies will play an important role in responding to Cyber Incidents through investigation, resources support, and resolution.

Cal-CSIC acts as the coordinating hub during the disruption, connecting affected entities with appropriate subject-matter experts to assist with resolution. When alerted to a cyber incident Cal-SCIC will help determine which State of California entity(s) will be involved in cyber response. Each of the primary State partners (California Governor’s Office of Emergency Services (Cal OES), California Highway Patrol (CHP), California Military Department (CMD), California Department of Technology (CDT) and the California Department of Justice (CA DOJ) operates within Cal-CSIC under the umbrella of its specific legal and regulatory authorities during an incident’s lifecycle. Cal-CSIC will maintain situational awareness and strategic oversight of the incident and act as an integration point for state and federal resource response and assistance.

Central California Intelligence Center (CCIC) provides cyber threat information and intelligence sharing, analysis, and dissemination between the federal, state, local, and private sector organizations, and incident response coordination in partnership with the County EOC. During a **SEVERE** Cyber Incident, the CCIC will have a seat within the EOC and may, upon request from either the Cyber IC or EOC Director, help to coordinate information requests and intelligence sharing.

The following Table 2 provides an overview of high-level responsibilities for each of the core groups:

Table 2: Cyber Incident Roles and Responsibilities

Organization	Overview
Department of Technology (DTech)	<ul style="list-style-type: none"> • Execute SIRP incident response activities. • Provide Cyber Incident Commander. • Determine Cyber Incident classification. • Serve as liaison to the EOC and CITF if activated • Make initial notifications to Government Response Organizations (CaISIC, CISA, and FBI). • Maintain contact with Departmental Information Security Officers and/or DOC(s) involved with response operations. • Coordinate the use of additional cybersecurity resources. • Provide ongoing situation status updates. • Maintain communication with County leadership. • Determine technical resources that may be needed.
Sac County OES	<ul style="list-style-type: none"> • Activate and manage the EOC.

Organization	Overview
	<ul style="list-style-type: none"> • Serve as the liaison between CITF, DTech, and staff functions. • Serve as the primary point of contact for Government Response Organizations during the response. • Coordinate public information releases, and the Joint Information Center for the incident. • Coordinate all county actions for mitigation to ensure continuity of government and critical services. • Keep County leadership and elected officials Informed. • Request and manage external resources. • Maintain situational awareness regarding impacts to IT Systems and operational impacts to Departments and Agencies. • Request mutual aid. • Activate the CITF.
<p>Departments and Agencies</p>	<ul style="list-style-type: none"> • Provide a representative to participate in the CITF. • Maintain accurate and timely inventories of IT Systems and operational limitations associated with the Cyber Incident. • Support DTech SIRP activities and response requirements • Develop mitigation strategies and requirements to maintain continuity of operations and services. • Consider COOP plan activation.
<p>Government Response Organizations</p> <ul style="list-style-type: none"> • CCIC • Cal-CSIC • CISA • FBI 	<ul style="list-style-type: none"> • Facilitate the exchange of law enforcement-sensitive threat intelligence information with State and Federal resources to support Cyber Incident response. • Collect and disseminate threat intelligence and investigative information. • Provide cybersecurity services, including cyber sensor monitoring, threat detection, incident investigation, incident response, forensics, and crisis management (as appropriate to the organization). • Provide access to contracted cyber security and IT incident response capabilities.
<p>Contracted Resources</p>	<ul style="list-style-type: none"> • Deliver contracted services, such as threat hunting, forensics, remediation, staff augmentation, and general IT operational capabilities as needed. • Provide replacement equipment, such as laptops, desktops, servers, switching equipment, and associated services.

2.6 Public Information Release

The release of information to the public will play an important role during a Cyber Incident. The EOC will coordinate with all involved departments, stakeholders, and partners to ensure accurate, timely, and transparent information is released regarding the incident.

Upon activation of the EOC the senior Public Information Officer for the County should be immediately notified and determine if a public statement is needed and/or a Joint Information Center (JIC) should be established to support the incident response. The Public Information Officer and/or JIC shall coordinate the content and release of all public information to external stakeholders including employees, affected agencies and people, the public, and the media.

The PIO/JIC should follow the County's existing crisis communication plans to guide the release of information about the Cyber incident.

An initial public information release to the impacted County population should go out as soon as possible and on-going updates should be released as more information becomes known. The initial release should include the following elements:

- Initial facts known regarding the incident
- Impacted systems and or people, if appropriate and does not compromise any response efforts or investigation
- What action is being done taken to resolve the incident
- Where to get more information regarding the incident

A final release should be sent upon resolution of the incident. All information released should be clear about the impacts of the incident, consider both internal and external stakeholders and use plain easy to understand language.

3.0 INCIDENT RESPONSE

The following section will describe incident response processes, phases, and key activities, which will be used to respond to a Cyber Incident. During a Cyber Incident, DTech will address the impacts to IT Systems through its SIRP processes. The primary goals in the SIRP are to stop the Cyber Incident and to restore IT Systems and data, which enable the operations of Sacramento County Departments and Agencies. In parallel with DTech's recovery efforts, this section outlines the response activities overseen by Sac County OES and the EOC to mitigate the impacts on County operations and services. The activities and actions outlined below may be implemented in whole or in part depending on the nature of the Cyber Incident and the needs of the County. This is to provide maximum flexibility to the Cyber IC and the EOC Director in responding to a Cyber Incident.

3.1 Process Overview

The EOC's actions will support and be consistent with the NIST 4-Step Security Incident Response Cycle process which will also be used by DTech to resolve the Cyber Incident. These four phases are summarized in Table 3 below.

Table 3: Cyber Incident Phases and Objectives

PHASE	OBJECTIVE
1. Preparation	<ul style="list-style-type: none"> Develop and maintain this Annex together with the skills to implement it in the event of a Cyber Incident.
2. Detection and Analysis	<ul style="list-style-type: none"> Support the needs of DTech in its activities in accurately detecting the Cyber Incident and analyzing artifacts and other information necessary to understand the likely impacts. Sac County OES, Departments and Agencies gather relevant information related to the impact on IT Systems.
3. Containment, Eradication and Recovery	<ul style="list-style-type: none"> DTech stops an attack, removes the threats to IT Systems and restores operations and data. Sac County OES, Departments, and Agencies understand operational impacts and mitigate them until IT Systems and data are restored with a return to normal operations.
4. Post Incident Review	<ul style="list-style-type: none"> Identify lessons learned, implement enhancements to processes and technology related to the Cyber Incident and continue learning with training and exercises.

3.2 Step 1: Preparation

In the Preparation Phase of Cyber Incident response, DTech has primary operational responsibility for hardening IT Systems and implementing and operating information security controls to prevent Cyber Incidents and mitigate their impacts.

As part of this Annex, all other organizations are responsible for on-going planning, training, and exercising their relevant response operations to Cyber Incidents. Sac County OES is the lead organization for ensuring that County Departments and Agencies perform relevant preparation activities.

3.3 Preparation Phase Responsibilities and Actions

Organization/Role	Responsibilities & Actions
DTech	<ul style="list-style-type: none"> • Appoint a principal liaison to the Incident Commander, their staff, and the CITF during a Cyber Incident. • Participate in CITF exercises, trainings, and reviews of the Cyber Hazard Annex. • Regularly exercise the SIRP. • Develop and maintain a disaster recovery plan for Sacramento County, including prioritization and restoration of systems and data when multiple Departments and Agencies are impacted in a Cyber Incident. • Conduct periodic risk assessments of critical systems to identify risks requiring mitigation and associated mitigation strategies. • Maintain cyber security systems and processes to reduce the likelihood and impacts of a Cyber Incident. • Participate in regional and national meetings to maintain situational awareness of developing trends and attacks. • Continuously evaluate systems for indicators of compromise as they become known.
Sac County OES	<ul style="list-style-type: none"> • Appoint an individual to lead the EOC and the CITF. The ideal candidate for the CITF lead would be knowledgeable in cyber incident response and IT operations. • Pre-designate CITF members from County Departments and Agencies. • Regularly convene the CITF to review the Cyber Hazard Annex. • Regularly exercise the Cyber Hazard Annex. • Ensure that COOP plans reflect disruptions from Cyber Incidents. • Maintain and exercise alternative means of communications to be used during a Cyber Incident.

Organization/Role	Responsibilities & Actions
	<ul style="list-style-type: none"> • Participate in regional and national meetings to gather best practices in emergency management of Cyber Incidents.
<p style="text-align: center;">All County Departments and Agencies</p>	<ul style="list-style-type: none"> • Provide a representative to the CITF. • Participate in the CITF to review the Cyber Hazard Annex. • Participate in exercises of the Cyber Hazard Annex. • Periodically review with all organizations within the Department or Agency that the COOP plans accurately reflect mission essential functions and capabilities. • Ensure that alternative means of communication channels are understood, and associated contact lists are kept up to date. • Participate in regional and national meetings offered through Sac County OES to maintain situational awareness of developing cyber trends and attacks.
<p style="text-align: center;">Public Information Officer</p>	<ul style="list-style-type: none"> • Maintain familiarity with this Cyber Hazard Annex, COOP plans and the SIRP. • Update and include communication templates regarding Cyber Incidents into the County's Crisis Communication Plan. • Participate in training and exercises related to Cyber Incidents. • Maintain contact lists and communications templates to enable contact with internal and external stakeholders through alternative means. • Develop communications templates for reasonably anticipated response events associated with a Cyber Incident.
<p style="text-align: center;">County Legal Team</p>	<ul style="list-style-type: none"> • Maintain familiarity with this Cyber Hazard Annex, COOP plans, and the SIRP. • Participate in training and exercises related to Cyber Incidents. • Maintain contact lists and communications templates to enable contact with internal and external stakeholders through alternative means.

3.4 Step 2: Detection and Analysis

During the Detection and Analysis Phase of a Cyber Incident, DTech will be primarily concerned with collecting information related to prospective or confirmed Cyber Incidents. These will include routine events that do not constitute High or Severe Cyber Incidents.

In the case of **HIGH** or **SEVERE** Cyber Incidents, the intensity of DTech activities is likely to be elevated, resulting in less time available to incident management and more uncertainty. In executing the SIRP, additional resources are likely to be required. In addition, engagement with intergovernmental partners at the State and Federal level is also likely. During this phase of activity, Cyber Incidents may manifest themselves through impacts to IT Systems and disruption to County Department and Agency activities.

During this phase, DTech will be primarily guided by the SIRP for its activities, supplemented by the actions and considerations found in this Annex. Sac County OES, Departments and Agencies, and others will be guided by this Annex. The EOC shall utilize the checklist and other tools contained in Appendices A – H in this Annex.

3.5 Detection and Analysis Phase Responsibilities and Actions

Organization/Role	Responsibilities & Actions
DTech	<ul style="list-style-type: none"> • Execute required activities provided in the SIRP • Notify the EOC in cases of High or Severe Cyber Incidents as defined in the SIRP and activate this Annex as appropriate. • Notify or coordinate with the EOC to notify, and update as needed, Government Response Organizations. • Identify and activate external support resources. • Collect forensic artifacts as appropriate to the Cyber Incident.
Sac County OES	<ul style="list-style-type: none"> • Activate the EOC at Level 4/Duty Officer level to maintain situational awareness • Participate in DTech-led Cyber Incident response calls/meetings. • Contact key staff and CITF members to prepare for possible activation. • Collect Cyber Incident information at regular intervals and post to WebEOC or alternative systems or tools. • Coordinate with DTech to ensure that Government Response Organizations are informed of the Cyber Incident. • Coordinate with DTech to establish a regular update schedule for both internal staff and relevant Government Response Organizations as appropriate. • Consider testing alternative means of communication • Review COOP plans.
All County Departments and Agencies	<ul style="list-style-type: none"> • Evaluate and maintain awareness of any impacts of the Cyber Incident on Department or Agency operations. • Provide updates to the EOC of any operational impacts.

Organization/Role	Responsibilities & Actions
	<ul style="list-style-type: none"> Participate in CITF briefings, updates, and meetings and communicate relevant details to the Department or business unit.
Public Information Officer	<ul style="list-style-type: none"> Evaluate and maintain awareness of any impacts of the Cyber Incident on County operations. Determine and continuously assess whether communications to internal or external groups is appropriate. Develop appropriate talking points for County leaders regarding the Cyber Incident. Develop an on-going communications plan and messaging update cadence. Participate in CITF briefings, updates, and meetings and otherwise maintain situational awareness related to the Cyber Incident. Reach out to County Department and Agency PIO's to coordinate activities and prepare for possible JIC activation.
County Legal Team	<ul style="list-style-type: none"> Take steps to assert privilege over communications and incident data collection as appropriate. Review regulatory and reporting requirements that may be triggered by the Cyber Incident. Participate in CITF briefings, updates, and meetings and otherwise maintain situational awareness related to the Cyber Incident.

3.6 Additional Responsibilities and Actions Required for Severe Cyber Incidents

The declaration of a **SEVERE** Cyber Incident means that significant disruptions to County Department and Agency operations have or are likely to occur. This is most likely to occur during the Detection and Analysis phase of response or after.

Organization/Role	Responsibilities & Actions
DTech	<ul style="list-style-type: none"> If not already done, notify the EOC of the occurrence of a Severe Cyber Incident. Assess the impacts to IT Systems and make initial estimates for recovery times. Update any prior notifications to relevant Government Response Organizations. Identify and activate external support resources.

Organization/Role	Responsibilities & Actions
Sac County OES	<ul style="list-style-type: none"> • Conduct a full activation of the EOC to level 1 or 2 • Activate the CITF and conduct an initial briefing for key EOC staff and CITF members. • Set CITF meeting schedule and agenda • Test and ensure that alternative means of communication channels are available. • Ensure that relevant Government Response Organizations are informed of the Cyber Incident. • Evaluate the need for County Departments and Agencies to activate COOP plans.
All County Departments and Agencies	<ul style="list-style-type: none"> • Make initial assessments of mitigation requirements and resources required to restore critical services. • Coordinate with the PIO (and JIC) to notify relevant stakeholders and constituencies of County service impairments and disruptions. • Test and ensure that alternative means of communication channels are available. • Participate in CITF briefings, updates, and meetings and communicate relevant details to the Department or Agency.
Public Information Officer	<ul style="list-style-type: none"> • Implement an internal and external communications plan to create appropriate awareness among internal staff and County citizens, partners, and other stakeholders. • Provide support to Departments and Agencies in messaging and communications content. • If the EOC is activated to a Level 1, activate a JIC.
County Legal Team	<ul style="list-style-type: none"> • Assess legal risk associated with significant disruption of County operations and create mitigation strategies. • Determine if breach notifications may be required and begin preparations for required notifications.

3.7 Step 3: Containment, Eradication and Recovery

Action described in this section are applicable to **HIGH** and **SEVERE** Cyber Incidents. If during this phase the incident is escalated from a **HIGH** to a **SEVERE** Cyber Incident, ensure that the relevant steps for Severe Cyber Incidents in section 3.3.2 are also performed.

During the Containment and Eradication period, this Annex describes the on-going management of operational impacts and required coordination activities. As the Cyber Incident moves to the Recovery period, mitigation

activities should continue as needed, but actions associated with planning for and transition to more a normal operational state are performed. These latter steps should be done consistent with the County EOP’s EOC deactivation criteria.

3.8 Containment and Eradication Phase Responsibilities and Actions

Organization/Role	Responsibilities & Actions
DTech	<ul style="list-style-type: none"> • Implement relevant actions required under the SIRP. • Assess the impacts to IT Systems and make initial estimates for recovery times and communicate those times to the EOC. • Develop and maintain a timely inventory of IT Systems and capabilities impaired by the Cyber Incident. • Consider implementation of the Disaster Recovery Plan and execute as appropriate. • Activate alternative means of communication channels if required. • Identify and activate external support resources.
Sac County OES	<ul style="list-style-type: none"> • Maintain and communicate situational awareness regarding SIRP execution, Disaster Recovery Plan execution (if applicable), and the status/recovery expectations for impacted IT Systems. • Maintain and communicate situational awareness regarding Department and Agency operational limitations and service interruptions associated with the Cyber Incident. • Continue coordination efforts among impacted Departments and Agencies (and the CITF if activated) to support continuity of services including potential need for Departments to activate COOP plans. • Establish regular meeting schedules with Government Response Organizations to share situational awareness, gather relevant information and coordinate the delivery of support to Sacramento County. • Utilize alternative means of communication channels if required.
All County Departments and Agencies	<ul style="list-style-type: none"> • Share situational awareness of operational impacts from the Cyber Incident with the EOC. • Develop and maintain a timely inventory of operational limitations and service interruptions associated with the Cyber Incident. • Provide on-going updates to the community and the EOC regarding operational limitations associated with the Cyber Incident. • Continue mitigating activities to support continuity of services.

Organization/Role	Responsibilities & Actions
	<ul style="list-style-type: none"> Continuously evaluate whether activation of the Department COOP plans are indicated Utilize alternative means of communication channels if required.
Public Information Officer	<ul style="list-style-type: none"> Execute internal and external communications plans to maintain appropriate awareness among internal staff and County citizens, partners and other stakeholders. Provide support to Departments and Agencies in messaging and communications content.
County Legal Team	<ul style="list-style-type: none"> Maintain situational awareness and provide guidance on managing legal risks. Oversee breach notifications and compliance with associated legal requirements if applicable.

3.9 Recovery Phase Responsibilities and Actions

Organization/Role	Responsibilities & Actions
DTech	<ul style="list-style-type: none"> Implement relevant actions required under the SIRP. Develop detailed plans for the recovery of IT Systems. Communicate timing and associated requirements to the EOC, effected Departments and Agencies, and the CITF if activated. Update inventories of IT Systems and capabilities impaired by the Cyber Incident. Undertake restoration activities under the Disaster Recovery Plan if implemented. Transition from alternative means of communication channels if appropriate. Update status with relevant Government Response Organizations. Deactivate external support resources as appropriate.
Sac County OES	<ul style="list-style-type: none"> Coordinate with DTech to plan and set conditions for deactivation of the EOC and CITF. Wind down situational awareness efforts regarding SIRP execution, Disaster Recovery Plan activities (if applicable), and the status/recovery expectations for impacted IT Systems. Wind down situational awareness regarding Department and Agency operational limitations and service interruptions associated with the Cyber Incident.

Organization/Role	Responsibilities & Actions
	<ul style="list-style-type: none"> • Wind down coordination efforts among impacted Departments and Agencies (and the CITF if activated) regarding mitigation efforts. • Wind down regular meeting schedules with Government Response Organizations and transition on-going engagements to DTech. • Transition from alternative means of communication channels if implemented.
All County Departments and Agencies	<ul style="list-style-type: none"> • Share situational awareness of restoration of operations to a regular state. • Communicate service restoration timelines and any on-going limitations to the community and other relevant Sacramento County Departments. • Transition operational functions to a regular state and terminate COOP-related activities and mitigations as appropriate. • Transition from alternative means of communication channels if implemented.
Public Information Officer	<ul style="list-style-type: none"> • Conclude internal and external communications plans among internal staff and County citizens, partners, and other stakeholders. • Provide final support to Departments and Agencies in messaging and communications content.
County Legal Team	<ul style="list-style-type: none"> • Manage on-going legal efforts associated with the Cyber Incident.

3.10 Step 4: Post Incident Review

Organization/Role	Responsibilities & Actions
DTech	<ul style="list-style-type: none"> • Conduct an after-action review in accordance with the SIRP. • Participate in an after-action review of response activities under the Cyber Hazard Annex. • Update relevant plans to reflect lessons learned.
Sac County OES	<ul style="list-style-type: none"> • Conduct an after-action review of response activities under the Cyber Hazard Annex. • Update relevant plans to reflect lessons learned.
All County Departments and Agencies	<ul style="list-style-type: none"> • Participate in an after-action review of response activities under the Cyber Hazard Annex.

Sacramento County
Cyber Hazard Annex

Organization/Role	Responsibilities & Actions
	<ul style="list-style-type: none">• Review COOP plans if activated to incorporate lessons learned.• Update relevant plans to reflect lessons learned.
Public Information Officer	<ul style="list-style-type: none">• Participate in an after-action review of response activities under the Cyber Hazard Annex.
County Legal Team	<ul style="list-style-type: none">• Participate in an after-action review of response activities under the Cyber Hazard Annex.

4.0 CRITICAL CONSIDERATIONS

4.1 Critical Considerations

Each Cyber Incident is unique and requires consideration of a variety of factors to better respond to it. To support the best response, the following considerations are unique aspects of a Cyber Incident that should be reviewed during the various phases of a response by the EOC, Department and Agency staff, CITF participants, and other response personnel. Critical considerations are organized by the phases of a Cyber Incident and the relevant organizations likely to have response activities. Each County Department and Agency may develop its own set of unique critical considerations consistent with this Annex.

4.2 Preparation

Organization/Role	Considerations
DTech	<ul style="list-style-type: none"> • Implement pre-defined communications modalities so that all parties can communicate effectively in the event of a Cyber Incident. Where possible consider multiple channels, including Teams, GoToMeeting, or Webex, etc. • Develop pre-contracted resource providers to supplement DTech staff in responding to all aspects of a Cyber Incident, including forensic analysis and IT equipment vendors. • Assess and where appropriate identify clear mechanisms for staff to leverage cloud-based applications and services both from outside Sacramento County infrastructure and potentially using personal devices. • Maintain a list of Government Response Organization contacts that may offer aid and develop relationships before a cyber incident presents itself. • Conduct risk assessments associated with critical technologies to identify relevant needs for hardening and otherwise enhancing cyber security practices.
Sac County OES	<ul style="list-style-type: none"> • Periodically consider County-wide mitigation strategies, including procuring or adjusting coverage limitations for cyber risk insurance coverage. • Ensure relevant organizations periodically review and exercise existing plans, including the SIRP and Sacramento County and Department COOP plans to ensure they appropriately accommodate Cyber Incidents that precipitate potential action.

Organization/Role	Considerations
	<ul style="list-style-type: none"> • Procure and periodically test communication solutions, preferably an automated mass communication solution to ensure all staff are contactable over varied modalities.
All County Departments and Agencies	<ul style="list-style-type: none"> • Develop processes to utilize alternative means of communication in the event the Cyber Incident impairs systems and capabilities normally utilized to conduct routine Sacramento County operations.
Public Information Officer	<ul style="list-style-type: none"> • Ensure that the PIO and other communications team members have pre-defined the respective means of sharing information to keep community and other government organizations apprised of Cyber Incidents, including consideration of mass automated communications tools.

4.3 Detection and Analysis Phase

Organization/Role	Considerations
DTech	<ul style="list-style-type: none"> • Determine and continuously reassess what external resources are required to support detection response activities, including engagement with Government Response Organizations. • Continuously assess for spreading operational impacts to systems and data. • Determine if existing sensors and staff can adequately detect and gather necessary data to create awareness of the scope of a potential Cyber Incident. • Determine if existing sensors and staff can adequately gather and store necessary data and forensic information to support analysis requirements. • Attempt to correlate signatures and identified indicators of compromise with threat intelligence provided by third parties, including organizations such as CISA. • Ensure that forensic data is collected and stored safely during detection investigation to support subsequent analysis and for sharing with other responding organizations. • Ensure that timely reporting is made through pre-planned channels to Government Response Organizations. • Determine if external digital forensic team deployment is required.

Organization/Role	Considerations
	<ul style="list-style-type: none"> • Determine if and how forensic data can be shared for supporting analysis by other responding organizations. • Continuously evaluate whether and to what extent a potential Advanced Persistent Threat (APT) is extant in Sacramento County systems. • Continuously evaluate to what extent sensitive information may have been compromised.
Sac County OES	<ul style="list-style-type: none"> • Determine as rapidly as possible the scope and impact of the potential incident, including continuously reassessing the Cyber Incident to determine the appropriate level and intensity of response. • Assess the workload of and coordinate with DTech staff to determine if coordination with Government Response Organizations is best coordinated by the EOC to free DTech staff for tactical level incident response activities. • Ensure that the occurrence of High and Severe Cyber Incidents are broadly communicated to Departments as early as practicable to enable early response activities. • Determine and continuously reassess what external resources are required to assist in Department mitigation activities as well as DTech response. • Continuously evaluate whether the business impacts of the Cyber Incident merit EOC and CITF activation. • Track possibly High and Severe Cyber Incidents by gathering relevant information. • Identify a consistent DTech staff member to gather information for shared situational awareness with Departments. • Ensure that communications to DTech staff by outside agencies are managed to ensure that Cyber Incident response activities are not impaired. • Evaluate that mass communications tools perform and operate as expected.
All County Departments and Agencies	<ul style="list-style-type: none"> • Verify that communications intended for staff, municipalities, and community organizations operate as expected. • Continuously evaluate whether alternative means of communications channels should be used.
Public Information Officer	<ul style="list-style-type: none"> • Ensure that status reports and information shared with PIO staff are technically accurate and do not include speculation regarding the Cyber Incident.

Organization/Role	Considerations
	<ul style="list-style-type: none"> • Ensure that accurate information regarding impacts to Sacramento County Department operations are clearly identified to support external communications. • Ensure that PIO and other communications staff have relevant access to DTech staff to ensure that messages and sharing of information is technically accurate.

4.4 Containment, Eradication, and Recovery Phase

Organization/Role	Considerations
DTech	<ul style="list-style-type: none"> • With new information discovered during this phase, verify that the correct root cause was determined, and eradication activity is reasonable to permanently remove the threat from IT Systems. • Continuously update threat intelligence sources for Indicators of Compromise (IOC) and forward the list to other entities with an advisory. • Verify with the EOC that there are appropriate resources available to perform eradication activities. • Determine which systems or processes are mission critical and prioritize them to be restored first. • Obtain a list of systems to be restored and their prioritizations • Ensure that users will be available to test their access and last good transaction in their systems once IT has restored them or access to them. • Identify any user accounts that were deactivated during analysis and set timings to reactivate the accounts and notify the users. • Determine if existing systems will be reused after eradication / sanitizing them or if new systems need to be sourced as replacements.
Sac County OES	<ul style="list-style-type: none"> • Determine as rapidly as possible the scope and impact of the potential incident, including continuously reassessing the Cyber Incident to determine the appropriate level and intensity of response. • Determine and continuously reassess what external resources are required to assist in Department mitigation activities as well as DTech response.

Organization/Role	Considerations
	<ul style="list-style-type: none"> Continuously evaluate whether the business impacts of the potential Cyber Incident merit EOC and CITF activation.
Public Information Officer	<ul style="list-style-type: none"> Ensure that status reports and information shared with PIO staff are technically accurate and do not include speculation regarding the Cyber Incident. Ensure that accurate information regarding impacts to Sacramento County Department operations are clearly identified to support external communications. Ensure that PIO and other communications staff have relevant access to DTech staff to ensure that messages and sharing of information is technically accurate.

Appendix A – Acronyms

CA-DOJ	California Department of Justice
Cal-CSIC	California Cyber Security Integration Center
CalOES	California Office of Emergency Services
CCRIC	Central California Regional Intelligence Center
CDT	California Department of Technology
CHP	California Highway Patrol
CITF	Cyber Incident Task Force
CIO	Chief Information Officer
CISO	Chief Information Security Officer (for Sacramento County)
COOP	Continuity of Operations
CMD	California Military Department
DHS	Department of Homeland Security
DOC	Department Operations Center
DTECH	Sacramento County Department of Information Technology
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
FBI	Federal Bureau of Investigation
IC	Incident Commander
JIC	Joint Information Center

NIST	The National Institute of Standards and Technology (U.S. Department of Commerce)
REOC	(Cal OES) Regional Emergency Operations Center
OES	Sacramento County Office of Emergency Services
SCADA	Supervisory Control and Data Acquisition
SIRP	Security Incident Response Plan
SIRT	Security Incident Response Team
SOC	DTech Security Operations Center

Appendix B – EOC Cyber Incident Checklist

#	Tasks
Detection & Analysis Phase	
<input type="checkbox"/>	Gather preliminary Cyber Incident information from DTech using the Cyber Incident Notification Form (Appendix D).
<input type="checkbox"/>	Activate EOC in support of a declared Cyber Incident
<input type="checkbox"/>	Notify key staff of the Cyber Incident and EOC activation status: <ul style="list-style-type: none"> • PIO • Legal • Sac County OES list
<input type="checkbox"/>	Notify CITF members with initial details of the Cyber Incident.
<input type="checkbox"/>	Gather initial status of impacts to Departments and Agencies using the Cyber Incident Notification Form (Appendix D). Gather restoration estimates from DTech.
<input type="checkbox"/>	Consult with DTech to determine what Government Response Organizations have and should be notified. Establish a regular meeting cadence as appropriate. Support notifications as directed by DTech.
<input type="checkbox"/>	Post relevant information to WebEOC.
<input type="checkbox"/>	Establish a regular briefing schedule for the CITF as directed by the EOC Director or designee.
<input type="checkbox"/>	Determine what, if any, contracted resources are required by DTech or Departments and Agencies in responding to the Cyber Incident.
<input type="checkbox"/>	Notify PIO and determine if a Joint Information Center (JIC) should be established to support public information.

<input type="checkbox"/>	Review alternative means of communication information and means for functionality.
Containment, Eradication, and Recovery	
<input type="checkbox"/>	Regularly update information and create situational awareness for the CITF and other stakeholders, including: <ul style="list-style-type: none"> • DTech response activities and understanding of the Cyber Incident • Status of Disaster Recovery Plan activities if implemented • Updated effected IT System and associated recovery time estimates • Operational impacts on CITF members and their mitigation measures • Government Response Organization notification and engagement
<input type="checkbox"/>	Conduct regular briefings of the CITF and other EOP stakeholders.
<input type="checkbox"/>	Coordinate among CITF members to identify needed resources to mitigate operational impacts of the Cyber Incident.
<input type="checkbox"/>	Coordinate with and support DTech to procure contracted resources.

Appendix C – EOC Cyber Incident Essential Elements of Information

Essential Elements of Information (EEI) provide information for situational awareness and decision-making. EEI must be verified and include specific details. The EEI are listed below by relevant community lifeline and by County Departments but are not all-inclusive.

Safety and Security

- Availability of 911 system to the public and responders.
- Limitations on critical business functions and services of County Departments and Agencies.
- Status of Sheriff's Department facilities.
- Limitations on Sheriff's Department activities.
- Status of Metro Fire facilities.
- Limitations on Metro Fire activities (including providing emergency medical services).
- Status of flood control facilities, including pumping stations.
- Limiting factors or obstacles for each entity's restoration of functions (sequencing of activities).
- Status of mutual assistance, major restoration efforts underway, and estimated times for restoration.

Health and Medical

- Status of critical healthcare facilities and services (hospitals, nursing homes, dialysis).
- Information on at-risk populations with access and functional needs and their medical and social service needs.
- Identifying and reporting emerging public health concerns.
- Status of garbage and waste collection.

Communications

- Status of 911 and Dispatch.
- Status and availability of County e-mail.
- Status and availability of County phone service.
- Ability of the County to issue alerts, warnings, and messages to County employees and the public.

Transportation

- Critical needs of materials, transportation, and physical access restrictions per sector.
- Status and availability of airport, seaport, and other transportation infrastructure.

All County Departments and Agencies

- What operational capabilities in serving constituents or customers have been impacted?
- Which of these capabilities are considered mission critical?
- Which of these capabilities are classified as critical infrastructure under Department of Homeland Security guidance?
- To what extent have capabilities been limited?
- What mitigations are in place to minimize the loss or limitation of capabilities?
- To what extent are staff able to work?
- What communications to constituents and customers have occurred?
- Will/Has the Department's or Agency's COOP Plan be/been activated?

DTech

- What systems are impacted?
- What is the nature of the Cyber Incident?
- Are there indications of on-going persistence mechanisms in systems?
- Are there indications of data exfiltration or other likely unauthorized access?
- What is the expected order of recovery of impacted systems and capabilities?
- What are the recovery time estimates for impacted systems?
- What are the expected losses of data based on backup recovery points?

Appendix D – Cyber Incident Notification Form

Date	MM/DD/YYYY						
Identification Time	HH/MM [AM/PM] [TZ]						
Physical Location	[Location] City, State						
Description							
<p><u>Source of Notification:</u> How was the event discovered?</p> <p><u>Known Impacts on County operations and function:</u> What services and capabilities are impacted. For how long?</p> <p><u>Incident Summary:</u> A brief explanation of the incident describing what is known, response actions taken, any tasks assigned and to whom they were assigned, and a general description of the plan to investigate.</p>							
Business Impact							
DTech Incident Severity Rating							
Type of Incident (select one)							
<input type="checkbox"/>	Common Malware	<input type="checkbox"/>	Phishing Attempt	<input type="checkbox"/>	Compromised Public Host	<input type="checkbox"/>	Backdoor
<input type="checkbox"/>	Advanced Threat	<input type="checkbox"/>	Violation of Acceptable Use	<input type="checkbox"/>	Unauthorized Network Activity	<input type="checkbox"/>	Unauthorized Software
<input type="checkbox"/>	Denial of Service	<input type="checkbox"/>	Controlled Data Spill	<input type="checkbox"/>	Lost/Stolen Laptop	<input type="checkbox"/>	Other

If other, explain	There may be situations when the process of investigation is required to determine the type of incident. This field should be used to provide a description of those events.
Supporting Details	
Use this space to describe, in detail, the investigation.	
Conclusions and Recommendations	
Use this space to describe remedial activities.	

Appendix E – Contact List Government Response Organizations

Organization	Primary Contact	Email	Phone
California Cybersecurity Integration Center (Cal-CSIC)			24-Hour Line: 916-845-8911 833-737-6781
US Secret Service			
CISA			
FBI	Sean Ragan SCIC		916-746-7000
Multi-State Information Sharing and Analysis Center (MS-ISAC)			
State Terrorism Assessment Center (STAC)		STAC@caloes.gov	916-636-2900
Sacramento Regional Threat Assessment Center (SacRTAC)			888-884-8383

Appendix F – Vendors

Vendor	Primary Contact / Support	Email	Phone
Cisco			
Microsoft			

Appendix G – CITF Points of Alternative Contact Means

Department	Representative	Email	Phone

Appendix H – IT System Outage Scorecard

Department	Affected Function	Outage Began	Estimated Time for Restoration	Outage Duration

Appendix I – Major Cyber Threat Actors and Attack Methods

Table 1: Major Cyber Threat Actors

Threat Actors	Description
Terrorists	Terrorists may use phishing schemes or spyware/malware and other attack methods to disrupt or disable critical infrastructure, or to steal funds, or sensitive information.
Cyber Criminals	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime also pose a threat through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent. Their goals are profit-based. Their sub-goals include attacks on infrastructure for profit to competitors, theft of trade secrets, and to gain access, and blackmail affected industry through public exposure.
Foreign Governments	<p>These actors usually involve the intelligence services of foreign governments that use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities.</p> <p>Threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Their goal is to weaken, disrupt, or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the U.S. economy, and full-scale attack of U.S. infrastructure when attacked by the U.S.</p>
Hactivists	Hactivists include individuals and groups, e.g., Anonymous, with anti-U.S. motives, or other political agendas. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause.
Hackers	<p>Hackers are often categorized as follows:</p> <ul style="list-style-type: none"> • Script kiddies are unskilled attackers who do not have the ability to discover new vulnerabilities or write exploit code and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages. • Worm and virus writers are attackers who write the propagation code used in the worms and viruses, but not typically the exploit code used to penetrate the systems infected. Their goal is

	<p>notoriety. Their sub-goals are to cause disruption of networks and attached computer systems.</p> <ul style="list-style-type: none"> • Security researcher and white hat have two sub-categories: bug hunters and exploit coders. Their goal is profit. Their sub-goals are to improve security, earn money, and achieve recognition with an exploit. • Professional hacker-black hat who gets paid to write exploits or actually penetrate networks; also falls into the two sub-categories- bug hunters and exploit coders. Their goal is profit.
Bot-network Operators	<p>Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).</p>
Insiders	<p>The disgruntled insider is a principal source of computer crime. This could be a full or part-time employee or contractor. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system, or to steal system data. The insider threat also includes individuals who <i>accidentally</i> introduce malware or spyware into systems.</p>
Phishers	<p>Individuals, or small groups, execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.</p>
Spammers	<p>Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).</p>
Spyware and Malware Authors	<p>Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.</p>

Table 2: Major Cyber Attack Methods

Attack Methods	Description
Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources, or the delaying of system operations and functions.
Telephone Denial of Service	Attacks that clog phone lines and interrupt regular phone usage and business with a flood of false call traffic.
Doxing	The collection and unauthorized release of personally identifiable information to the public. This may include all relevant personal details, such as name, address, phone numbers, date of birth, Social Security Number, social networking information, usernames, passwords, images, and anything else that is related to a person in an identifying capacity.
Phishing	A digital form of social engineering that uses authentic-looking—but phony—emails to request information from users or direct them to a fake website that requests information.
Ransomware	Ransomware is a form of malware in which rogue software code effectively holds a user's computer hostage until a "ransom" fee is paid. Ransomware often infiltrates a computer as a computer worm or Trojan horse that takes advantage of open security vulnerabilities. The Port of San Diego was hit by a ransomware attack in September 2018 which adversely impacted a variety of port functions.
Watering Hole Attack	Tactics that combine social engineering and malware to target specific individuals at companies or government agencies by infecting legitimate and frequently visited websites and exploiting holes in browser software systems with the goal of stealing trade or other secrets.
Virus	A hidden, self-replicating section of computer software, usually malicious logic, which propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.
Worms	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.
Trojan Horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
Super Cyber Weapons	Cyber-attack methods so sophisticated they require a government sponsor to develop and deploy them, e.g., the Stuxnet Virus. Such weapons are often deployed against other governments in order to conduct intelligence gathering and/or sabotage.