Grand County
Colorado

GRAND COUNTY CYBER INCIDENT RESPONSE PLAN

Approved and adopted by Grand County Chief Information Security Officer (CISO) on 01-DEC-2021

Table of Contents

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK)

1 INTRODUCTION

Since 2010 there has been an increased frequency and voracity of cybersecurity-related attacks within the United States of America. These attacks have damaged and/or disrupted Federal, State, and Local government services and have stolen countless volumes of confidential, personal, and financial information to support criminal endeavors. These disruptions and thefts have cost American institutions and citizenry a tremendous amount of loss. Cybersecurity-related attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when a security breach occurs. The concept of cyber incident response has become widely accepted to establish capability within and organization to respond to cyber incidents in a systematic way so that the appropriate actions are taken.

The purpose of the Grand County Cyber Incident Response Plan is to establish cyber incident response capabilities and handle cyber incidents efficiently and effectively to mitigate losses from successful cybersecurity-related attacks.

1.1 Cyber Incident Classification

A Cyber Incident (Type 1) is an adverse event or group of events which impact the confidentiality, integrity, or availability of information systems, services, networks, or policies used by Grand County. Examples of Cyber Incidents include, but are not limited to:

- Loss of a Grand County device
- Misuse of Grand County service, systems, or information
- Hacking, attempts to steal passwords, or other malicious activity
- Damage to systems from malicious code attacks (i.e. Viruses, Trojans, etc.)

A Significant Cyber Incident (Type 2) is defined as an event this is likely to cause, or is causing, harm by impairing the confidentiality, integrity, or availability of information, systems, services, or networks which threaten public safety, undermine public confidence, or diminish cybersecurity readiness and require multiple Grand County Offices or Departments to be involved in coordination and integration with outside agencies or entities to successfully respond and recover from.

Examples of significant cyber incidents may include, but are not limited to; public safety communications; emergency response capability; drinking water; energy delivery; telecommunication systems; and critical infrastructure and key resources (CIKR) sectors within the County of Grand.

A Significant Cyber Incident requires additional organization and coordination as define in the Grand County Significant Cyber Incident Annex.

1.2 Incident Response Team

Figure 1 Incident Response Team Relationships

The Incident Response Team (IRT) is a group of individuals trained to respond to cyber incidents. The IRT provides both an investigative and problem-solving component as depicted in Figure 1. The IRT includes leadership with the authority to act, technical resources with the knowledge and expertise to rapidly diagnose and recover from cyber incidents. The initial IRT is comprised of the Grand County Manager, Chief Information Security Office, Information Systems department, and Incident Reporter. IRT membership may be expanded as appropriate and will include, at a minimum, the Grand County Office of Emergency Management Director during a Significant Cyber Incident.

2 INCIDENT RESPONSE TEAM STRUCTURE

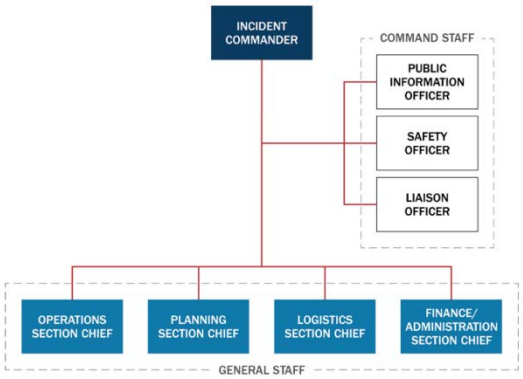


Figure 2 Incident Command Structure (ICS)

The team structure utilized during a Cyber Incident will be the Incident Command Structure (ICS) as depicted in Figure 2 as defined in the National Incident Management System (NIMS) maintained by the Federal Emergency Management Agency (FEMA). The actual roles utilized will be determined based on the Cyber Incident Classification. Using this structure Grand County should be able to transition both efficiently and effectively when/if the situation warrants participation by outside agencies.

2.1 Initial Assignments for a Type 1 Incident

Below are the primary and secondary resources that will be initially assigned a role within the IRT during a non-Significant Cyber Incident.

Position	Primary	Secondary
Incident Commander	Chief Information Security Officer	Emergency Management Director
Public Information Officer	N/A	N/A
Liaison Officer	County Manager	Assistant County Manager
Operations Section Chief	InfoSys Supervisor	InfoSys Administrator
Planning Section Chief	Chief Information Security Officer	InfoSys Supervisor
Logistics Section Chief	N/A	N/A
Finance Section Chief	N/A	N/A

2.2 Initial Assignments for a Type 2 Incident

Below are the primary and secondary resources that will be initially assigned a role within the IRT during a Significant Cyber Incident.

Position	Primary	Secondary
Incident Commander	Emergency Management Director	External Agency Representative
Public Information Officer	Communications Director	External Agency Representative

Position	Primary	Secondary
Liaison Officer	County Manager	External Agency Representative
Operations Section Chief	InfoSys Supervisor	External Agency Representative
Planning Section Chief	Chief Information Security Officer	External Agency Representative
Logistics Section Chief	Emergency Management Deputy	External Agency Representative
Finance Section Chief	Finance Director	Finance Supervisor

3 ROLES & RESPONSIBILITY

Below is a brief summary of responsibilities by role during a Cyber Incident. The role listing is not exhaustive and additional roles may be defined as the situation warrants. For additional details on the responsibilities please reference Chapter III of the National Incident Management System (NIMS).

Role	Responsibility
Incident Commander	Responsible for the overall management of the incident. Establishes consolidated objectives, priorities, and updates them every operational period.
Public Information Officer	Responsible for the interfaces with the public, media, and/or other agencies with incident-related information.
Liaison Officer	Point of contact for representatives of governmental agencies and organizations outside of the IRT.
Operations Section Chief	Direct the management of tactical activities on behalf of the Incident Commander. Develop and implement strategies and tactics to achieve objectives.
Planning Section Chief	Responsible for the collection, evaluation, and dissemination of situation information to the Incident Commander and incident personnel. Facilitate the incident action planning process and facilitate meetings.
Logistics Section Chief	Responsible for providing support services for effective and efficient incident management, including ordering resources.
Finance Section Chief	Responsible for recording personnel time, administering claims, and tracking and analyzing incident costs.

4 CYBER INCIDENT INFORMATION SHARING

Media and/or Public information releases will be coordinated with the Public Information Officer and require Incident Commander clearance prior to release.

Partner/Vendor/Agency releases will be coordinated with the Liaison Officer and require Incident Commander clearance prior to release.

Each Section Chief will provide at least hourly status updates to the Planning Section Chief who in turn will disseminate the information to the Incident Commander and incident personnel.

The following default meeting schedule will be utilized until adjusted by the Incident Commander:

Meeting	Time	Purpose
Command Objectives Meeting	07:00	Share updated information to facilitate the General Meeting.
Morning Meeting	08:00	Provide current status and direction to staff.
Tactics Meeting	09:00	Develop primary and alternate strategies/ to meet Incident Objectives for the next operational period.
Media Briefing	10:00	Provide a status briefing to the media
Planning Meeting	16:00	Review status and finalize strategies/tactics and assignments to meet Incident Objectives for the next operational period and get tacit approval of plan.
Incident Briefing Published	17:00	Publish the Incident Briefing (ICS 201) to the incident personnel
Operations Briefing	18:00	Present plan and assignments to the supervisors/leaders for the next operational period.

5 CYBER INCIDENT COMMUNICATION & COLLABORATION TECHNOLOGIES

Below are the accepted communication and collaboration technologies to be utilized, with primary being the preference for Type 1 incidents and as solutions for any gaps not provided by an external controlling agency.

Purpose	Primary	Secondary
All Staff Notification	Service Desk Notifications Desktop Notifications SMS Gateway	Word of mouth Manager phone tree
IRT Chat	Google Chat Space https://www.co.grand.co.us/IRTChat	WebEx Teams External Agency Provided
IRT Conference	Google Meet https://www.co.grand.co.us/IRTConference	WebEx Meeting External Agency Provided

Purpose	Primary	Secondary
IRT Web Portal	Google Site https://www.co.grand.co.us/IRTWebPortal	External Agency Provided
IRT File Share	Google Drive https://www.co.grand.co.us/IRTFileShare	External Agency Provided
Incident Management System	IRT Web Portal & File Share	External Agency Provided

6 CYBER INCIDENT RESPONSE LIFE CYCLE

The diagram in Figure 3 depicts the high-level work flow of an incident with the specific tasks and activities within the "Detection & Analysis" and "Containment, Eradication, & Recovery" phases being iterative until recovery has been successfully achieved.

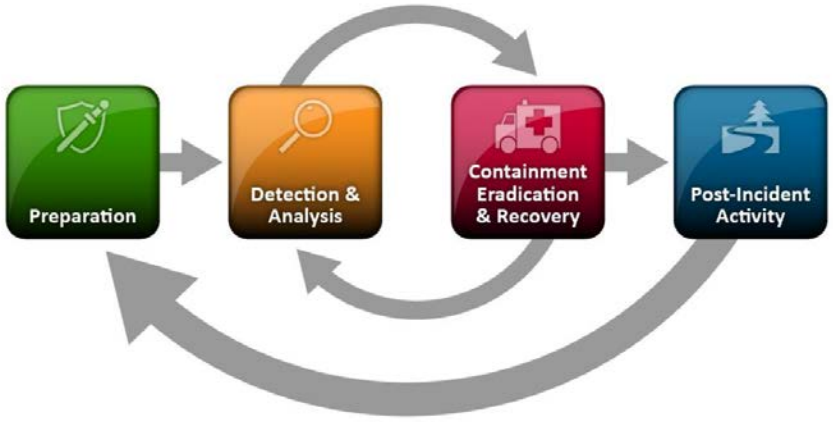
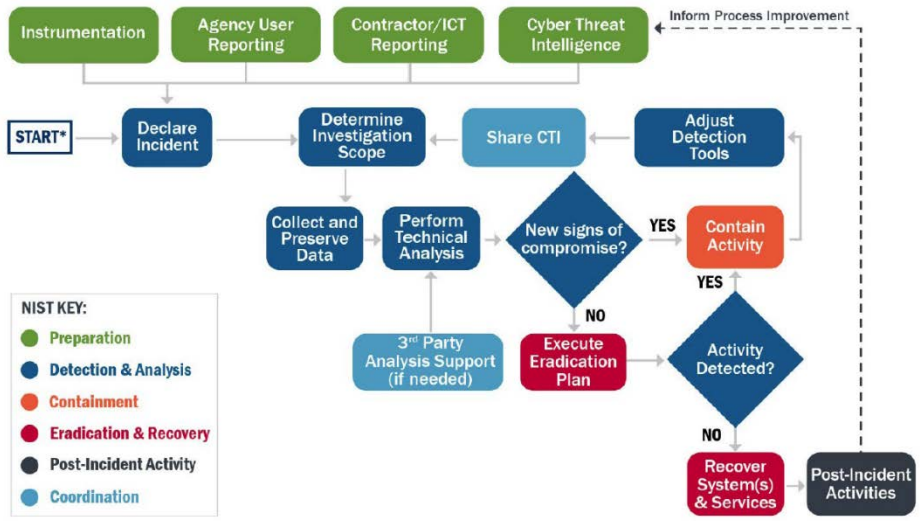


Figure 3 Cyber Incident Response Life Cycle

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Different types of incidents will require different response strategies. The "Preparation" phase of the lifecycle is outside the scope of this document and is considered an aspect of normal operations.

7 CYBER INCIDENT RESPONSE PROCESS



The diagram in Figure 4 identifies the specific activities, decisions, and relationships within the Cyber Incident Response Process. Detailed information is supporting these activities are supplied in later sections within this document.

Figure 4 Cyber Incident Response Process

8 CYBER INCIDENT DETECTION & ANALYSIS

8.1 Detection & Reporting

There is a wide array of sources for precursors and/or indicators of an incident. The most important activity is reporting the information so that a determination on the risk can be obtained and the appropriate next action defined. There are three acceptable methods (in order of preference) to report suspected cyber incident indicators, they are:

- Sending a detailed email to the Grand County Help Desk at support@co.grand.co.us
- Completing the Information Security Concern Form at https://www.co.grand.co.us/IRTConcern
- Calling the Grand County Help Desk:
  - During business hours at +1-970-725-3825
  - Outside of business hours at +1-970-250-0197

8.2 Cyber Incident Type Declaration

The Grand County Chief Information Security Officer (CISO) will determine the incident classification in accordance with guidance described in paragraph 1.1 above and using the Impact Analysis Form located at https://www.co.grand.co.us/IRTImpact. Once the Threat Scope is known and the Incident Type identified, the Grand County CISO will notify the appropriate Incident Commander so that they may begin organizing the IRT.

8.2.1 Initial Organization Steps of IRT

The Incident Commander will ensure the following activities are completed to activate the IRT:

1. Assemble the IRT as prescribed by paragraph 2 above.
2. Establish an organizing meeting with the IRT via Google Meet.
3. Provide notification of activation of the IRT within IRT Chat.
4. Conduct backup isolation/validation analysis to determine if immediate evasive tasks are needed.
5. Begin construction of ICS 201 (Incident Briefing)
6. Provide initial notification of threat to Grand County management and staff.
7. Provide initial notification to external agencies and partners, as appropriate.

8.3 Analysis

8.3.1 Determine Investigation Scope

Once an incident has been declared, the next step is to establish the scope of the investigation required to reasonably determine the type of access, extent to which assets have been affected, and organizational impact of the adversarial activity.

1. Use the aforementioned Impact Analysis Form as a starting point.
2. Determine what additional data is required to determine type, extent, and impact.
3. The investigation scope has now been established, update the ICS 201.
4. Proceed to Collect and Preserve Data activities.

8.3.2 Collect and Preserve Data

Data is collected and preserved to support incident verification, categorization, prioritization, mitigation, reporting, attribution, and as potential evidence. The data collected is informed by the investigation scope and can included, but not limited to, the following:

- Data from the perimeter, internal network, and endpoint.
- Audit, transaction, intrusion, connection, system performance, and user activity logs.
- Forensic captures of memory and disk images and/or backups.

When necessary and possible, the data collected should be preserved and safeguarded for potential use in law enforcement investigations. The following items should be logged for all evidence collected:

- How the evidence was collected.
- When the evidence was collected.
- Who collected the evidence.

8.3.3 Perform Technical Analysis

As data and evidence is collected it will be analyzed to develop a technical and contextual understanding of the incident to inform containment, eradication, and restoration activities. Technical Analysis is complete when the following objectives are satisfied:

- The incident has been verified (i.e. real and impactful).
- The incident scope has been determined.
- The method(s) of persistent access have been identified.
- The impact of the incident has been assessed.
- A hypothesis has been constructed which includes a narrative and associated Tactics, Techniques, and Procedures (TTP) and Indicators of Compromise (IOC).

Upon completion of the initial Technical Analysis, proceed to Containment activities.

8.3.4 Adjust Detection Tools

As adversarial TTP's and IOC's are identified the IRT will update the appropriate tools to improve prevention and detection capabilities.

9 CYBER INCIDENT CONTAINMENT, ERADICATION, & RECOVERY

9.1 Containment

The objective of containment is to prevent further damage and reduce the immediate impact of the incident by removing the adversary's access. The containment strategies employed will be driven by the specific incident. Containment is considered completed when the following objectives are satisfied:

- There are no new signs of compromise (i.e. adversary access has been removed).

- Evidence is preserved for reference and law enforcement investigation.
- Detection and protection tools have been adjusted and updated.

Upon completion of Containment, proceed to Eradication.

9.1.1 Containment Strategies & Criteria

During an incident one or more containment strategies can be used to remove the adversary's access. Below are some key containment strategies; this list is NOT all inclusive. To determine the appropriate strategies to employ consider the following:

- Requirements to preserve evidence
- Availability of services
- Resource constraints
- Speed of containment

Containment Strategy	Criteria for Usage
Block (and log) network traffic	Used to block connectivity and communication to an IP, port, or domain used by an adversary.
Change passwords	Used to deny authentication when credentials have been compromised and though to be in use by an adversary.
Executable Blocking/Blacklisting	Used to block an executable from running through the use of filenames and/or hashes.
Isolate affected systems and networks	Used to remove network access from a compromised asset by removing interface, cable, or VLAN assignment.
Prevent DNS resolution	Used to modify DNS resolution to direct communication to a sinkhole or sandbox.
Revoke privileged access	Used to revoke access by disabling an account or updating security groups of a compromised account.
Rotate private keys	Used to revoke the decryption ability by an adversary when a private key is compromised.
Shutdown system	Used to revoke control and usage of a compromised system by an adversary.
Stop and disable Services	Used to terminate a service or daemon that is being used by an adversary for communication and/or control of a compromised asset.

During containment activities you should monitor for signs of adversary response to the containment in an attempt for the adversary to maintain access. If there are responses which maintain access, then you will need to conduct additional technical analysis to determine additional containment responses.

9.2 Eradication

The objective of this phase is to allow the return of normal operations by eliminating artifacts of the incident (e.g., remove malicious code, re-image infected systems) and mitigating the vulnerabilities or

other conditions that were exploited. Before moving to eradication, ensure that all means of persistent access into the network have been accounted for, that the adversary activity is sufficiently contained, and that all evidence has been collected. This is often an iterative process. It may also involve hardening or modifying the environment to protect targeted systems if the root cause of the intrusion and/or initial access vector is known. It is possible that eradication and recovery actions can be executed simultaneously.

1. Develop an eradication plan that considers use of alternative attack vectors and multiple persistence mechanisms.
2. Continually provide incident status updates as eradication activities are conducted.
3. Ensure evidence and data are collected, if needed, prior to conducting eradication activities.
4. Conduct eradication activities, such as:
    a. Removal of artifacts of the incident from affected systems and assets.
    b. Reimage affected systems from clean backups, baseline images, or OEM sources.
    c. If firmware or hardware rootkits are involved, rebuild or replace hardware.
5. Conduct configuration hardening of system or asset.
6. Install current patches, updates, hot-fixes, and/or workarounds.
7. Scan for malware to ensure removal of malicious code.
8. Update security tools with appropriate TTP's and IOC's.
9. Monitor to ensure adversarial persistence has been removed.
10. If no new adversary activity is discovered, continue to Recovery; else return to Technical Analysis.

9.3 Recovery

The objective of this phase is to restore systems to normal operations and confirm they are functioning normally. A key aspect of recovery is to also have enhanced vigilance and controls in place to validate that the recovery is successful and that there are no signs of adversary activity in the environment.

1. Install and configure additional required software (i.e. applications and databases).
2. Install current patches, updates, hot-fixes, and/or workarounds.
3. Validate system and software configuration and security controls.
    a. If possible, emulate adversarial TTP's to verify countermeasure and/or monitoring are effective.
4. Restore and validate organizational data (i.e. files, databases, etc.)
5. Functionally test systems thoroughly to validate they are operating normally.
6. Release system for normal usage.
7. Closely monitor environment for evidence of threat actor activity.

10 POST-INCIDENT ACTIVITIES

The objective of this phase is to document the incident, inform leadership, and identify lessons learned to improve detection and response in future incidents. Activities in this phase include:

- Provide post-incident updates as required by law and policy.
- Publish a post-incident report that addresses the Who, What, Where, Why, and How questions.
- Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.
- Identify and address operational "blind spots" to coverage moving forward.
- Identify any policies and procedures updates to improve organizational capabilities and/or prevent similar incidents from occurring.
- Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.
- Identify evidence retention and disposal, as appropriate.

11 APPENDIX A: CONTACT LIST

Agency	When to contact
Grand County Manager	Always
Grand County Clerk & Recorder	Election related/impacted incidents

Table 1 Internal Agency Contacts

Agency	Email	Phone	Local	State	Federal
MS-ISAC	soc@msisac.org	866.787.4722	Y		
Colorado Office of Info Security	infosec@state.co.us			Y	
Colorado Secretary of State		303.894.2200		Y	
CISA	central@cisa.gov	888.282.0870			Y

Table 2 External Agencies & Partners

12 APPENDIX B: ONLINE RESOURCES

- IRT Web Portal
  - https://www.co.grand.co.us/IRTWebPortal
- IRT Chat
  - https://www.co.grand.co.us/IRTChat
- IRT Conference
  - https://www.co.grand.co.us/IRTConference
- IRT File Share
  - https://www.co.grand.co.us/IRTFileShare
- Information Security Concern Form
  - https://www.co.grand.co.us/IRTConcern
- Impact Analysis Form
  - https://www.co.grand.co.us/IRTImpact
- MITRE ATT&CK®
  - https://attack.mitre.org/
- MITRE ATT&CK® Navigator
  - https://mitre-attack.github.io/attack-navigator/

13 APPENDIX C: REFERENCES

- Grand County Information Security Manual
- Grand County Significant Cyber Incident Annex
- National Incident Management System (NIMS) Third Edition, October 2017.
- CISA Cybersecurity Incident & Vulnerability Response Playbooks, November 2021.
- NIST SP 800-61 Revision 2, August 2012.
- NIST SP 800-83 Revision 1, July 2013.