COMMISSIONER MEETINGS
All meetings take place in the Commissioners Conference Room (3107)
located in City Hall @ 316 North 26th Street (3rd Floor)
and are open to the public unless otherwise noted

THURSDAY - OCTOBER 23, 2025

8:45 Calendar

9:00 COMMISSIONERS DISCUSSION

PLEDGE

DEPARTMENTS

1. **Elections -** Broadview and Laurel Ballots
2. **County Attorney -** Attorney Referral Program
3. **IT -** Adoption of Yellowstone County Incident Response Plan and Incident Response Playbook

COMMISSIONERS

1. Commissioner Board Reports

PUBLIC COMMENTS ON COUNTY BUSINESS

Public comment is an opportunity for individuals to address the Board, however, the Board cannot engage in discussion or take action on items not properly noticed on the agenda.

CLOSED: STDF Security

B.O.C.C Thursday Discussion 1.

Meeting Date: 10/23/2025

Title: Elections - Broadview and Laurel Ballots

Submitted By: Erika Guy

TOPIC:

Elections - Broadview and Laurel Ballots

BACKGROUND:

NA

RECOMMENDED ACTION:

Discuss

B.O.C.C Thursday Discussion 2.

Meeting Date: 10/23/2025

Title: Attorney Referral Program

Submitted For: Amy Tolzien Submitted By: Amy Tolzien

TOPIC:

County Attorney - Attorney Referral Program

BACKGROUND:

Attorney Referral Program was approved by BOCC on December 13, 2022. We are updating the procedure to include all YCAO employees with the exception of the elected official.

RECOMMENDED ACTION:

Discuss & add to Consent Agenda.

Attachments

Atty Referral

Yellowstone County Attorney's Office (YCAO)
Attorney Referral Program

YCAO is continually looking for skilled prosecutors and recognizes that its current employees are a valuable resource in recruiting talented and experienced professionals to join its ranks.

The Attorney Referral Program will provide a monetary bonus to currently employed YCAO employees who successfully refer qualified candidates to the YCAO for employment.

* Bonus up to $4000 *

Bonus amount per referred attorney candidate:

1. $1,000 within 30 days of the referred candidate's start date with YCAO;
2. $1,000 within 30 days of the referred candidate's completion of the six-month probationary period; and,
3. $2,000 within 30 days of the referred candidate's completion of one year of employment.

Rules and Guidelines:

1. A written referral form provided by Yellowstone County must be submitted to the County Attorney and Human Resources before a qualified candidate's interview to be considered for a referral bonus. Hiring of the candidate must occur within three months of receipt of the written referral form.

2. All employees currently employed by YCAO are eligible for the bonus program.

3. Referral bonuses will be awarded on a first-submitted basis of the written referral form.

4. Rehires are eligible as successful referral candidates for this program only if they have been separated from YCAO for at least 18 months.

5. Referrals for part-time attorney positions may result in a prorated award.

6. There is no limit to the number of referral bonuses an employee may receive.

7. A referring employee must be actively employed by YCAO at the time of payment. Termination of employment by the referring employee before the bonus is fully paid will result in the forfeiture of any remaining unpaid bonus.

8. All referred candidates will be evaluated for employment per Yellowstone County and YCAO hiring practices.

9. Referral bonuses will be processed through the Yellowstone County payroll system and included in the employee's paycheck. Bonuses are subject to all legally required tax withholdings and deductions.

10. Any disputes or interpretations related to this referral program will be handled through Human Resources and the County Attorney.

11. The Attorney Referral Program will operate as long as there exists more than one open attorney position. An attorney resignation letter received by the County Attorney or Human Resources may be considered an opening for purposes of the referral program.

12. The Board of County Commissioners may cancel the Attorney Referral Program at their discretion. All referral bonuses associated with the employment of a referred candidate prior to the program's cancellation will be honored in full.

B.O.C.C Thursday Discussion 3.

Meeting Date: 10/23/2025

Title: Adoption of County Incident Response Plan & Incident Response Playbook

Submitted For: Larry Ziler, IT Director Submitted By: Larry Ziler, IT Director

TOPIC:

IT - Adoption of Yellowstone County Incident Response Plan and Incident Response Playbook

BACKGROUND:

The Incident Response Plan outlines a structured, county-wide approach to identifying, managing, and recovering from cybersecurity incidents. It defines roles, responsibilities, escalation paths, and communication protocols to ensure swift and coordinated action across departments. The Incident Response Plan has been reviewed and approved by necessary department heads and employees. Their input ensures the documents reflect operational realities and support a coordinated, county-wide approach to incident response.

The accompanying Incident Response Playbook provides detailed, scenario-based guidance for responding to specific types of incidents—such as ransomware, data breaches, or system outages. These playbooks translate policy into action, enabling technical teams and leadership to respond decisively and consistently under pressure.

???????Formal adoption by the Board of County Commissioners is essential for several reasons:

- Authority and Accountability: Adoption establishes the plan and playbook as official county policy, empowering staff to act decisively and ensuring leadership oversight.
- Cross-Departmental Alignment: It signals unified commitment across all departments, reinforcing collaboration and shared responsibility in incident response.
- Regulatory and Legal Readiness: Many cybersecurity frameworks and insurance providers require documented, board-approved response protocols. Adoption strengthens the County's compliance posture.
- Public Confidence: Demonstrating preparedness and governance reassures residents that Yellowstone County takes cybersecurity seriously and is equipped to protect public assets and services.

RECOMMENDED ACTION:

As the IT Director for Yellowstone County, MT; I respectfully recommend the Board of County Commissioners formally adopt the proposed Incident Response Plan and Incident Response Playbook as official county policy.
Larry P. Ziler
IT Directory
Yellowstone County, MT

Attachments

County Incident Response Plan

County Incident Response Playbook

Incident Response Plan

Version 1.1

Version History

Version	Date	Author	Reason/Comments
1.1	September 2023	Jim Nelson, Jeff Slavick	Initial review
1.1	May 2024	Jim Nelson	Initial Review continued
1.1	April 2025	Jim Nelson / Steve Yogodzinski	Final Review for approval
1.2	August 2025	Larry Ziler	Review for Approval
1.3	September 2023	Larry Ziler	Revisions suggested by county leadership. Finance, CA,
1.4	October 2024	Larry Ziler	Final proofreading.
1.5	October 2025	Larry Ziler	Final Draft submit to BOCC

Contents

Introduction

The Yellowstone County Incident Response Plan has been developed to provide direction and focus to the handling of information security incidents that adversely affect Yellowstone County **Information Resources**. The Yellowstone County Incident Response Plan applies to any person or entity charged by the Yellowstone County Incident Response Commander with a response to information security related incidents at the organization, and specifically those incidents that affect Yellowstone County **Information Resources**.

The purpose of the Incident Response Plan is to allow Yellowstone County to respond quickly and appropriately to cyber security events and incidents.

Event Definition

Any observable occurrence in system, network, environment, process, workflow, or personnel. Events may or may not be negative in nature.

Adverse Events Definition

Events with a negative consequence. This plan only applies to adverse events that are computer security related, not those caused by natural disasters, power failures, etc.

Incident Definition

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations. A security incident may have one or more of the following characteristics:

A. Violation of an explicit or implied Yellowstone County security policy
B. Attempts to gain unauthorized access to a Yellowstone County Information Resource
C. Denial of service to a Yellowstone County Information Resource
D. Unauthorized use of Yellowstone County Information Resources
E. Unauthorized modification of Yellowstone County information
F. Loss of Yellowstone County Confidential or Protected information

Reference

- Blue Team Handbook: Incident Response Edition, Don Murdoch
- NIST SP800-61r2: Computer Security Incident Handling Guide

Contact Information

Name	Title	Role	Contact Information	Escalation (1-3)*
Larry Ziler	Information Technology Director	IR Commander, CSIRT manager	lziler@yellowstonecountymt.gov 406-696-9810	**1**
Melissa Williams	Chief Civil Attorney	Communications Lead	mwilliams@yellowstonecountymt.gov 406-256-2832	3
Steve Williams	In-House Counsel	Communications Assistance	swilliams@yellowstonecountymt.gov	3
FRSecure	3rd Party Support	Incident Response and Digital Forensic Investigation	CSRIT@FRSecure.com	3
Traveler's Insurance	3rd Party Support	Cyber Insurance	Travelers Claim: 800-842-8496 Marsh McLennan: Caitlin Finnicum Caitlin.Finnicum@MarshMMA.com 406-238-1996	3
Jen Jones	Finance Director	Cyber Insurance (Internal); Public Relations	jjones@yellowstonecountymt.gov	3

*Escalation level determines order in which notification should occur:

1. Notify first, required on all incidents.
2. Required on all moderate or high severity incidents.
3. Involve as needed.

Roles and Responsibilities

Information Technology Director

- Seek approval from Executive Management for the administration of the Incident Response Program.
- Coordinate response activities with auxiliary departments and external resources as needed to minimize damages to information resources.
- Ensure service level agreements with service providers clearly define expectations of the organization and the service provider in relation to incident response.
- Ensure policies related to incident response accurately represent the goals of the organization.
- Review the Cyber Security Incident Response Plan ("the Plan") to ensure that it meets policy objectives and accurately reflects the goals of the organization.
- Approve close of moderate or critical-severity incidents.
- Ensure lessons learned are applied/weighed based on risk for Severity 1 incidents.
- Assemble a Cyber Security Incident Response Team (CSIRT).
- Ensure personnel tasked with incident response responsibilities are trained and knowledgeable on how to respond to incidents.
- Update Plan and procedures as needed based on results from testing, incident response lessons learned, industry developments and best practices.
- Review the Plan and procedures at least annually.
- Initiate tests of the Plan and procedures at least annually.
- Ensure team activities comply with legal and industry requirements for incident response procedures.
- Act as the primary Incident Response Manager, responsible for declaring a cyber security incident, managing team response activities, and approving close of Severity 2 & 3 incidents.
- Be aware of Cyber Insurance Policies, contact mechanisms, and when to include providers. (See Appendix VIII)

Cyber Security Incident Response Team (CSIRT)

The CSIRT is comprised of IT management and experienced personnel. The role of the CSIRT is to promptly handle an incident so that containment, investigation, and recovery can occur quickly. Where third-party services are leveraged, ensure they are engaged as necessary.

Roles within the CSIRT include:

IR Commander

The incident response commander oversees and prioritizes actions during the detection, analysis, and containment of an incident. They are also responsible for conveying the special requirements of high severity incidents to the rest of the organization as well as communicating potential impact to the county commissioners. Additionally, they are responsible for understanding the SLAs in place with third parties, and the role third parties may play in specific response scenarios.

Incident Response Team Members

The Incident Response Commander is supported by a team of technical staff that work directly with the affected information systems to research the time, location, and details of an incident. Team members are typically comprised of subject matter experts (SMEs), senior level IT staff, third parties, outsourced security or forensic partners.

Further responsibilities:

- Assist in incident response as requested. CSIRT responsibilities should take priority over normal duties.
- Understand Yellowstone County incident response plan and procedures to appropriately respond to an incident.
- Continue to develop skills for incident response.
- Ensure tools are properly configured and managed to alert on security incidents/events.
- Analyze network traffic for signs of denial of service, distributed denial of service, or other external attacks.
- Review log files of critical systems for unusual activity.
- Monitor business applications and services for signs of attack.
- Collect pertinent information regarding incidents at the request of the IR Commander.
- Consult with qualified information security staff for advice when needed.
- Ensure evidence gathering, chain of custody and preservation is appropriate.
- Participate in tests of the incident response plan and procedures.
- Be knowledgeable of service level agreements with service providers in relation to incident response.

Recorder

The Incident Response Commander may assign a team member to begin formal documentation of the incident.

Table 1: Anticipated (Company) CSIRT Team Members

No.	CSIRT Member	Role
1.	Larry Ziler	IR Commander –406-696-9810
2.	Jenna Masters	Network Administrator – jmasters@yellowstonecountymt.gov 406-208-7534
3.	Konnie Rutherford	IT Senior Engineer 406-606-0396
4.	Will Grimm	IT Specialist – wgrimm@yellowstonecountymt.gov 406-998-4309
5.	Ken Twichel	Phone Systems - ktwichel@yellowstonecountymt.gov 406-208-1780

6.	Laura Grieshop	Systems Administrator - lgrieshop@yellowstonecountymt.gov 406-894-0291
7.	Jamie DeBree	Web and Database Administrator – jdebree@yellowstonecountymt.gov 406-256-2761

Incident Response Framework

Yellowstone County recognizes that, despite reasonable and competent efforts to protect **Information Resources**, a breach or other loss of information is possible. The organization must make reasonable efforts and act competently to respond to a potential incident in a way that reduces the loss of information and potential harm to customers, partners, and the organization itself.

Developing a well-defined incident response framework is critical to an effective incident response plan. The Yellowstone County incident response framework is comprised of six phases that ensure a consistent and systematic approach.

Phase I – Preparation

It is essential to establish a Cyber Security Incident Response Team (CSIRT), define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools. (See Phase I – Preparation)

Phase II – Identification and Assessment

Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legislative and legal requirements. (See Phase II - Identification and Assessment)

Phase III – Containment and Intelligence

Containment of the incident is necessary to minimize and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties. (See Phase III – Containment and I)

Phase IV – Eradication

Eradication requires removal or addressing of all components and symptoms of the incident. Further, validation must be performed to ensure the incident does not reoccur. (See Phase IV – Eradication Details)

Phase V – Recovery

Recovery involves the steps required to restore data and systems to a healthy working state allowing business operations to be returned. (See Phase V – Recovery Details)

Phase VI – Lessons Learned

The Lessons Learned phase includes post-incident analysis on the system(s) that were impacted by the incident and other potentially vulnerable systems. Lessons learned from the incident are communicated to executive management and action plans developed to improve future incident response practices and reduce risk exposure. (See Phase VI - Lessons Learned)

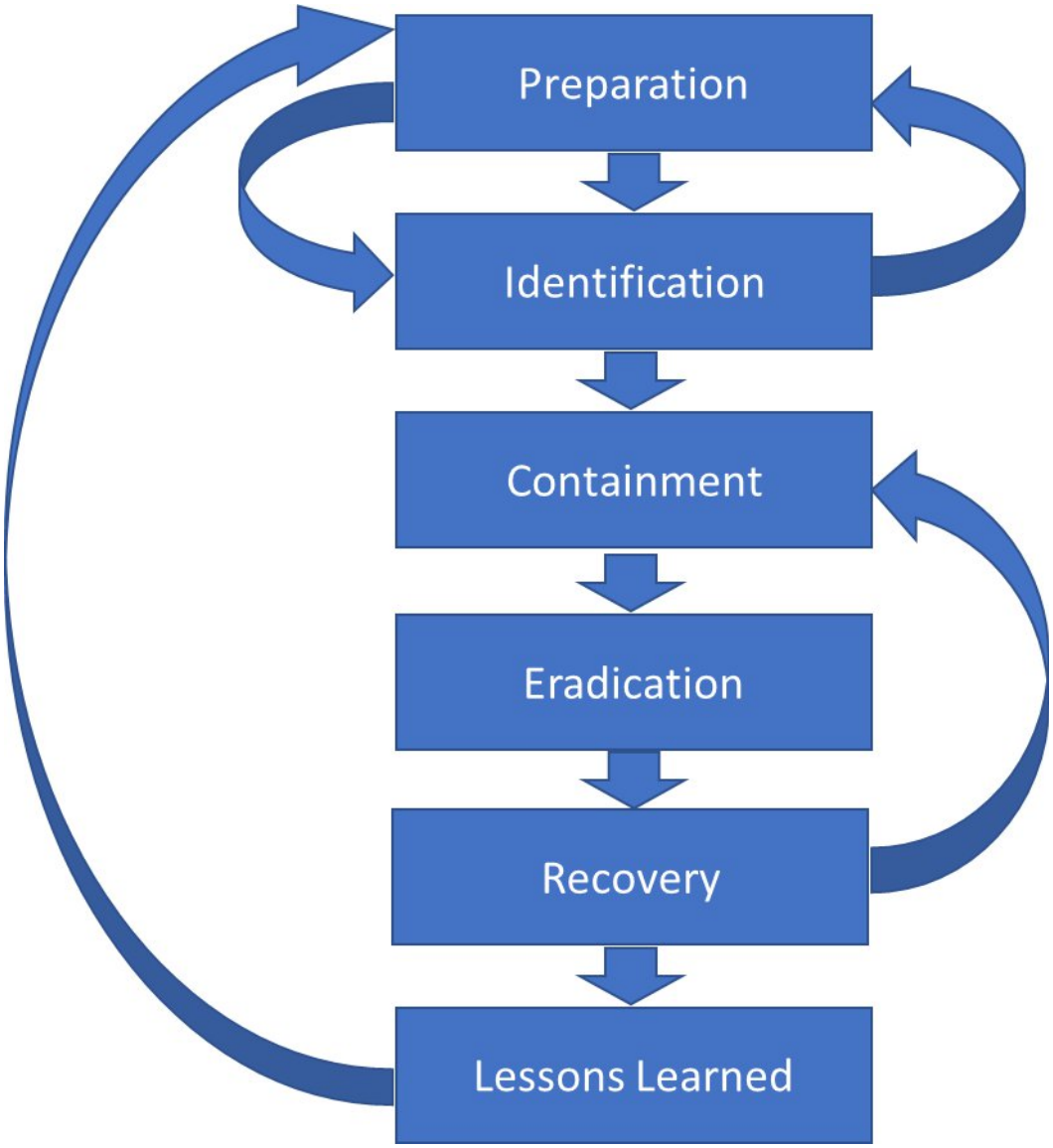


Figure 1:PICERL Framework Model

Reference

- SANS PICERL Incident Response Model

Phase I – Preparation

The Preparation phase is easily the most important phase. Without proper preparation incident response activities may be disorganized, expensive, and could cause irreparable harm to Yellowstone County.

Tasks included in the Preparation phase include but are not limited to the following.

- Establish

- Cyber Security Incident Response Team (CSIRT).
- Ensure appropriate parties are aware of incident reporting processes. (See **Error! Reference source not found.**)
- Document and share cyber insurance details with appropriate parties. (See Appendix VIII)
- Validate Logging, Alerting, and Monitoring policy compliance.
- Ensure CSIRT receives appropriate training based on skill gap analysis, career development efforts, and skill retention needs.
- Ensure CSIRT has access to the tools and equipment needed based on estimated ROI and the organization's risk appetite.
- Define and document standard operating procedures and workflows for the CSIRT.
- Improve documentation, checklists, references, etc.
- Maintain and validate Network Diagrams and Asset Inventories.
- Review Penetration Test reports and validate remediations to findings.
- Review Vulnerability Management reports and validate remediation efforts.
- Establish disposable and disabled administrative credentials to be enabled and used for investigations.

Logging, Alerting, and Monitoring

Basic system and activity logging must be implemented prior to the onset of an event. Managed effectively; logging, alerting, and monitoring will enable event identification and provide valuable information to the CSIRT during containment, investigation, eradication, and recovery phases.

Logging, Alerting, and Monitoring activities should be established according to the requirements of the Vulnerability Management Policy and may require specific tools to be effective. Review and update the **Logging, Alerting, and Monitoring Activities List** regularly to ensure that the security monitoring is complete and effective.

A Logging Standard should be developed to ensure that all critical systems meet the logging requirements of the organization.

Logging should include:

- Abnormal system events.
- Changes to security parameter settings.
- Network configuration changes.
- All successful and unsuccessful login attempts.
- All remote access.
- All logoffs.
- All access to restricted information.
- All additions, deletions and modifications to user accounts, user privileges, access rules and permissions.

- Attempts to perform unauthorized functions, including unauthorized access attempts.
- All password changes.
- All activities performed by privileged accounts.
- All access to sensitive transactions.
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes.
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes.
- All server system startups and shutdowns.
- Application process startup, shutdown, or restart.
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault.
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

Cloud-specific logging:

- Management plane activities.
- Automated system activities.
- Cloud provider management activities.
- Network flow.

Logs should feed into a centralized log server or SIEM. Log aggregation and correlation is key in IR activities and will save your team valuable time and resources in the process of identification, containment, and eradication. Devices should be synchronized to the same time server to ensure that the times recorded across all logs are aligned.

Logs should be maintained for a minimum of 12 months, or as required by the Vulnerability Management Policy and Retention Standard. Where storage is limited or costly, logs older than 30 days may be moved to alternate, cheaper storage locations. Logs must be secure. Logs should be encrypted, protected with unique credentials, and write access restricted, where possible.

Alerting should be maintained according to an established baseline. Suspicious activities and changes in system performance should automatically alert team members for further review.

Monitoring consists of both human and machine/automated monitoring. Human monitoring involves assigning CSIRT members with monitoring responsibilities, such as reviewing logs and following up on alerts. Machine monitoring consists of advanced analysis, such as behavioral monitoring and anomaly detection. Regular monitoring additionally allows team members to become familiar with normal behaviors of networks, systems, and applications making it easier for them to recognize abnormal behavior.

Reporting Incidents

Effective ways for both internal and outside parties to report incidents is equally critical as sometimes users of Yellowstone County systems and information may be the first to observe a problem. Review the different types of incidents addressed in Phase II under

Incident Categorization and list or establish reporting methods for a variety of incident types.

Reporting Method	Available To	Incident Type	Anonymous	Response Time
Service Desk Plus: Trackable ticket generation – contact method via email or dedicated phone number to Help Desk team	Employees	All Incident Types	No	Immediate during office hours. Otherwise within 1 hour of open.
Larry P. Ziler406-696-9810	Employees	Off-hours Incidents	No	Immediate
Helpdesk	Employees	Off-hours Incidents	No	Immediate

Phase II - Identification and Assessment

Identification

When a Yellowstone County employee or external party notices a suspicious anomaly in data, a system, or the network, or a system alert generates an event, Security Operations, Help Desk, or CSIRT must perform an initial investigation and verification of the event.

Events versus Incidents

As defined above, Events are observed changes in normal behavior of the system, environment, process, workflow, or personnel. Incidents are events that indicate a possible compromise of security or non-compliance with Yellowstone County policy that negatively impacts (or may negatively impact) the organization.

To facilitate the task of identification of an incident, the following is a list of typical symptoms of security incidents, which may include any or all of the following:

A. Email or phone notification from an intrusion detection tool.
B. Suspicious entries in system or network accounting, or logs.
C. Discrepancies between logs.
D. Repetitive unsuccessful logon attempts within a short time interval.
E. Unexplained new user accounts.
F. Unexplained new files or unfamiliar file names.
G. Unexplained modifications to file lengths and/or dates, especially in system files.
H. Unexplained attempts to write to system files or changes in system files.
I. Unexplained modification or deletion of data.
J. Denial/disruption of service or inability of one or more users to login to an account.
K. System crashes.
L. Poor system performance of dedicated servers.
M. Operation of a program or sniffer device used to capture network traffic.
N. Unusual time of usage (e.g. users login during unusual times)
O. Unusual system resource consumption. (High CPU usage)
P. Last logon (or usage) for a user account does not correspond to the actual last time the user used the account.
Q. Unusual usage patterns (e.g. a user account associated with a user in Finance is being used to login to an HR database).
R. Unauthorized changes to user permission or access.

Although there is no single symptom to conclusively prove that a security incident has taken place, observing one or more of these symptoms should prompt an observer to investigate more closely. Do not spend too much time with the initial identification of an incident as this will be further qualified in the containment phase.

NOTE: Compromised systems should be disconnected from the network rather than powered off. Powering off a compromised system could lead to loss of data, information or evidence required for a forensic investigation later. ONLY power off the system if it cannot be disconnected from the wired and wireless networks completely.

Assessment

Once a potential incident has been identified, part or all of the CSIRT will be activated by the IR Commander to investigate the situation. The assessment will determine the category, scope, and potential impact of the incident. The CSIRT should work quickly to analyze and validate each incident, following the process outlined below, and documenting each step taken.

The Two-Minute Incident Assessment, found at Appendix II, should be leveraged to rapidly determine if further investigation is necessary. Further, it can be modified and used to report the incident to appropriate leadership as required.

The Incident Response Commander will assign a team member to be "Recorder" to begin formal documentation of the incident. The below determined categorization, scope, and impact must be included with documentation of the incident.

Incident Categorization

The MITRE ATT&CK Framework is a globally accessible knowledge base of adversary tactics and techniques and should be leveraged when categorizing security incidents. While many techniques may be used in a single incident, select the method that was primarily leveraged by the adversary. Some examples of this may be:

- Phishing
- Unsecured Credentials
- Network Sniffing
- Man-in-the-Middle
- Data Destruction
- OS Credential Dumping
- Event Triggered Execution
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Hijacking
- Defacement
- File and Directory Permissions Modification

It should be noted that the MITRE ATT&CK Framework may not address some situations, specifically those without malicious intent, that trigger the Incident Response Plan. The following exceptions may require categories of their own as dictated by the organization's Risk Management entities or policies:

- Data Loss
- Administrative Errors
- Lax File and Directory Permissions
- Cyber Security Policy Violations
- Accidental Data Destruction
- Resource Misuse (non-malicious)
- Network Interruption
- ADD OTHERS AS APPLICABLE TO THE ORGANIZATION/INDUSTRY

Incident Scope

Determining the scope will help the CSIRT understand the potential business impact of the incident. The following are some of the factors to consider when determining the scope:

- How many systems are affected by this incident?
- Is Confidential or Protected information involved?

- What is/was the entry point for the incident (e.g. Internet, network, physical)?
- What is the potential damage caused by the incident?
- What is the estimated time to recover from the incident?
- What resources are required to manage the situation?
- How could the assessment be performed most effectively?

Incident Impact

Once the categorization and scope of an incident has been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate the course of action to be taken in order to provide a resolution; however, in all instances an incident report must be completed and reviewed by the Incident Response Commander. Functional and informational impacts are defined with initial response activity below:

Functional Impact	Definition	CSIRT Response
None	No effect to the organization's ability to provide all services to all users.	Create ticket and assign for remediation.
Limited	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.	Create ticket and assign for remediation, notify the County Commissioners.
Moderate	The organization has lost the ability to provide a critical service to a subset of system users.	Initiate full CSIRT, involve the County Commissioners
Critical	The organization is no longer able to provide some critical services to any user.	Initiate full CSIRT and County Commissioners. Consider activation of the Disaster Recovery Plan

Informational Impact	Definition	CSIRT Response
None	No information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	No action required
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the data owners to determine the appropriate course of action.
Moderate	Internal Information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the County Commissioners. County Commissioners will work with management, legal, and data owners to determine appropriate course of action.
Critical	Protected Data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the County Commissioners. County Commissioners will work with legal to determine whether reportable, and the appropriate notification requirements.

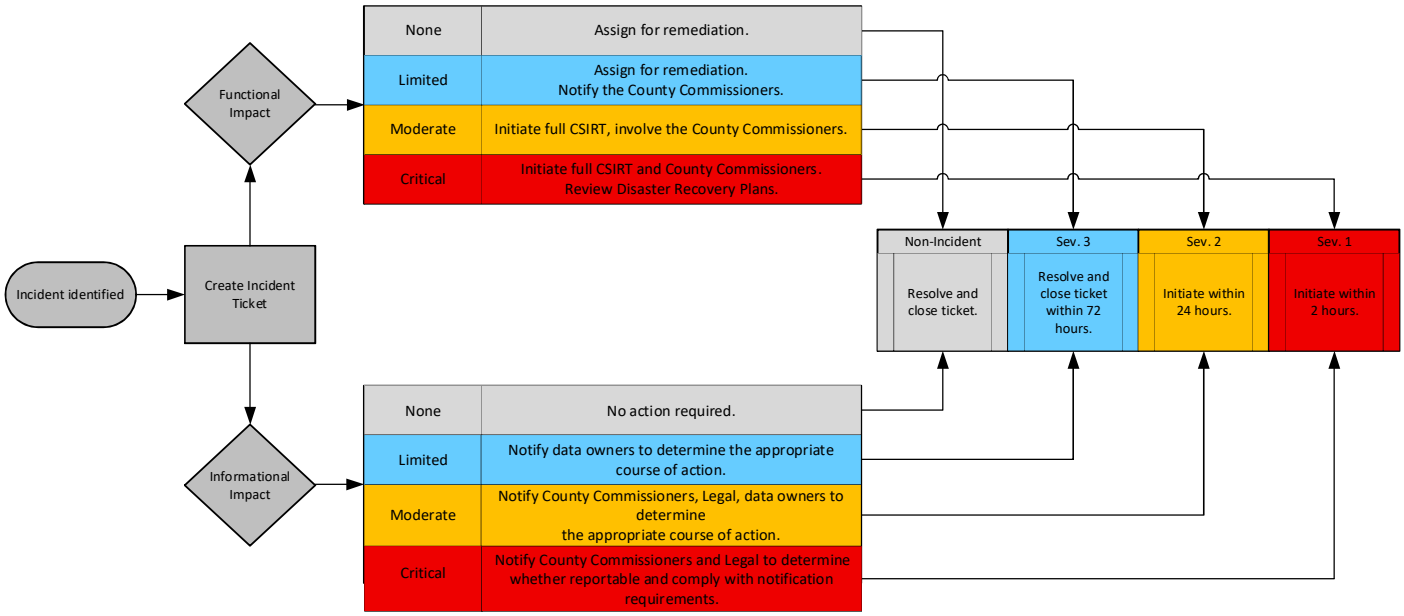
All incidents must be logged in the **Incident Handling Log & Assessment Tool**. A record of all action taken to remediate the incident, including chain of custody records, and deviations from SOP must be included in the documentation.

The **Incident Handling Log & Assessment Tool** and Response Level table below will help determine the severity of the incident and urgency of response activities.

Response Level Classification		**Informational Impact**			
		None	**Limited**	**Moderate**	**Critical**
Functional Impact	**None**	N/A	Sev. 3	Sev. 2	Sev. 1
	Limited	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	Moderate	Sev. 2	Sev. 2	Sev. 2	Sev. 1
	Critical	Sev. 1	Sev. 1	Sev. 1	Sev. 1

The severity level should be used to determine how rapidly initial response activities should occur.

Severity Level	SLA
Sev. 3	Within three days
Sev. 2	Within 24 hours
Sev. 1	Within 2 hours



CSIRT Assessment Communications and Insurance

1. Communications

Proper handling of internal and external communications is critical to successfully respond to a cyber security incident. The following communication issues should be considered.

a. **Attorney-Client Privilege/Attorney Work Product.** The County Commissioners and/or the IT Directory will consult with legal counsel to determine whether the investigation and response to a cyber security Incident should proceed under the direction of legal counsel and under attorney-client privilege, work product, and other applicable privileges. If so, the IT Director must follow all instructions of Legal and external legal counsel regarding Cyber security Incident-related communications.

b. **Internal Communications.** In accordance with the Yellowstone County Incident response Policy:

   i. Personnel should be notified whenever an incident or incident response activities may impact their work activities.

   ii. Internal communications should aim to avoid panic, avoid the spread of misinformation, and notify personnel of appropriate communication channels.

c. **External Communications.** In accordance with the Yellowstone County Incident response Policy, the Yellowstone County Attorney's Office/Steve Williams must coordinate all external communication.

2. Insurance

The County Commissioners, in coordination with the Chief Financial Officer of Yellowstone County, shall determine the scope of any applicable insurance coverage and, where appropriate, file a claim or notice of circumstances and utilize any available cyber-insurance resources.

Key Decisions for Exiting Identification and Assessment Phase:

- If the Identification and Assessment process has determined the event constitutes a real incident, the IR process must be continued.
- All details in the Identification phase must be documented in the Incident Reporting Form if the event is determined to be an incident.
- Communication and Cyber Insurance considerations have been made or revisited.

Examples of when to return to the Identification and Assessment Phase:

- The known scope of the incident is found to exceed expectations and reassessment is needed.

Phase III – Containment and Investigation

The objective of the containment phase of the incident response is to regain control of the situation and limit the extent of the damage. To achieve this objective, Yellowstone County has defined a number of containment strategies relevant to a variety of incident types. Reference the procedures related to one or more of the Containment Strategies listed below.

Containment Strategies

Use the list of strategies below to choose the procedure(s) most appropriate for the situation. Full procedures for the strategies can be found in the incident playbooks. If none of these strategies or playbooks match the current situation, refer to ***Common Containment Steps*** listed below.

- Stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks.
- Ransomware – isolate the impacted system, validate the ransomware claim, contact insurance carrier if impacted systems cannot be corrected, and identify whether additional systems have been impacted and isolate as needed.
- If DOS/DDOS - control WAN/ISP.
- Virus outbreak – contain LAN/system.
- Data loss – review user activity, implement data breach response procedures.

- Website defacement – repair site, harden from future attacks.
- Compromised API – review changes made, repair API, harden from future attacks.

The following Playbooks are available with the Yellowstone County Policy and Standards.

- Business Email Compromise
- Credential Theft
- Lost or Stolen Device
- Malware Outbreak
- Ransomware
- Web Application Compromise
- IR Lessons Learned Playbook (IRLLP)

Common Containment Steps

Containment requires critical decision making related to the nature of the incident. The Incident Response Manager, in coordination with the Incident Response Commander and other members of Executive Management, should review all the containment steps listed below to formulate a strategy to contain and limit damages resulting from the incident.

All attempts to contain the threat must consider every effort to minimize the impact to the business operations. Third party resources or interested parties may need to be notified. Where law enforcement may become involved, efforts must be made to preserve the integrity of relevant forensic or log data and maintain a clear chain-of-custody. Where evidence cannot be properly maintained due to containment efforts, the introduced discrepancy must be documented.

When evaluating containment steps, consider the following:

- Enable disposable administrative accounts for use during the investigation and reset associated passwords if believed to have been at risk of compromise while in being used. (See Phase I – Preparation)
- Will the ability to provide critical services be impacted? How? For how long?
- When should the Cyber insurance carrier be notified? (See Table 3: Insurance Coverage and Contact Information)
- Is a legal investigation or other action likely? Does evidence need to be preserved? (See Preserve Evidence)
- How likely is the containment step to succeed? What is the end result, full containment or partial?
- What resources are required to support the containment activity?
- What is the potential damage to equipment and other resources?

- What is the expected duration of the solution? (Temporary, short-term, long-term, or permanent)
- Should IR team members act discretely to attempt to hide their activities from the attacker?
- Is the assistance of a third party required? What is the expected response time?
- Do interested parties (customers, partners, investors) need to be notified? If so, when? (See Appendix IV)
- Does the impact to Yellowstone County equipment, network, or facilities necessitate the activation of the Disaster Recovery Plan?
- Does the data impacted include protected data such as cardholder data? If yes, refer to Notification Requirements.

Engage Resources

The CSIRT should select the option based on the severity of the incident, the damage incurred by Yellowstone County and legal considerations.

	In-house investigation	Law enforcement	Private forensic specialist
Time Response	Quick response	Varies by area and agency	Quick response
Competency	Skills vary	Depends on local law enforcement	Highly skilled, often with law enforcement background
Preservation of evidence	Does not ensure evidence integrity	Preserve evidence integrity and present evidence in court	Preserve evidence integrity and present evidence in court
Reputation impact	Minimal effect	Potential loss of reputation if certain incidents reach public	Potential loss of reputation if certain incidents reach public

Preserve Evidence

NOTE: Isolate compromised systems from the network. Avoid changing volatile state data or system state data early on (e.g. do not power off affected systems).

If there is strong reason to believe that a criminal or civil proceeding is likely, the Yellowstone County Chain of Custody form (location) must be used any time evidence has been taken into custody, or custody is transferred for the purpose of investigation. *For incidents involving cardholder data, Visa has defined specific requirements to be followed to preserve evidence and facilitate the investigation. Refer to Notification Requirements for more information.*

Consult legal counsel regarding applicable laws and regulations related to evidence collection and preservation. Create a detailed log for all evidence collected, including:

- Identification information (e.g. serial number, model, hostname, MAC address, IP address, or other identifiable details).
- Name and contact information for all individuals who have handled the evidence during the investigation.
- Date and time of each transfer or handling of the evidence.
- List of all locations where the evidence was stored.
- Deviations from SOP and associated justifications.

Follow guidance from NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, when preserving evidence.

Reduce Impact

Depending on the type of incident, the team must act quickly to reduce the impact to affected systems and/or reduce the reach of the attacker. Actions may include, but are not limited to the following:

- Stop the attacker using access controls (disabling accounts, resetting active connections, changing passwords, implementing router ACLs or firewall rules, etc.).
- Isolate compromised systems from the network.
- Avoid changing volatile state data or system state data early.
- Identify critical external systems that must remain operational and deny all other activity.
- Maintain a low profile, if possible, to avoid alerting an attacker that you are aware of their presence or giving them an opportunity to learn the CSIRT's tactics, techniques, or procedures.
- To the extent possible, consider preservation of system state for further investigation or use as evidence.

Collect Data and Increase Activity Logging

Increase monitoring and packet capture on affected systems while the CSIRT investigates the scope and impact of the incident. Continue increased logging and monitoring as you move onto the Eradication and Recovery phases.

- Enable full packet capture.
- Collect and review system, network, and other relevant logs.
- Create a memory image of impacted systems.
- Take a forensic image of affected systems.
- Monitor possible attacker communication channels.

Conduct Research

Performing an Internet search, consulting third party resources, and/or consulting IT Insurance carrier using the apparent symptoms and other information related to the incident you are experiencing may lead to more information on the attack. For example, if the insurance carrier has received multiple reports of similar incidents, or if a mailing list message contains the same IP or text of the message you received.

Notify Interested Parties

Once an incident has been identified, determine if there are others who need to be notified, both internal (e.g. human resources, legal, finance, communications, business owners, etc.) and external (e.g. service providers, government, public affairs, media relations, customers, general public, etc.). Always follow the "need to know" principle in all communications. Most importantly, remain factual and avoid speculation.

Depending on the degree of sensitivity of the incident, it may be necessary for Legal/Management to require employees to sign NDAs or issue gag orders to employees who need to be involved.

Investigation

As the CSIRT works to contain, eradicate, and recover from the incident, the investigation will be ongoing. As the investigation proceeds, you may find that the incident is not fully contained, eradicated, or recovered. If that is the situation, it may be necessary to revisit earlier phases (see Figure 1:PICERL Framework Model). The Containment, Eradication, and Recovery phases are frequently cyclical.

The investigation attempts to fully identify all systems, services, and data impacted by the incident, including root cause analysis, which helps to determine the entry point of an attacker or weakness in the system that allowed the event to escalate into an incident.

A third-party may need to be contracted if investigation is beyond the skills of the CSIRT, impacted systems are owned by a Cloud Service Provider, or forensic analysis is required.

Initial Cause ("Root Cause") Investigation

Investigation should be conducted with consideration given to the ongoing impact to critical business operations. Ideally, the Initial Cause Investigation should be concluded before leaving the Eradication phase. At times, however, it may be necessary or appropriate to continue investigation during or after eradication and recovery. Delaying the Investigation should only be considered when the CSIRT is confident that the incident has been fully contained and the full scope of the impact is known. Delays or modifications to the scope of investigation activities must be approved by the Incident Response Commander.

The investigation techniques utilized will vary by the type of incident. The investigation may rely on some (or all) of the following:

- Interviews with witnesses and/or affected persons.
- Capturing images, snapshots, or memory dumps of affected systems.
- Obtaining relevant documents.
- Conducting observations.
- Taking photographs of physical locations.
- Reviewing security camera footage.
- Analyzing the logs of the various devices, technologies and hosts involved (e.g. firewall, router, anti-virus, intrusion detection, host).
- Reviewing email rules (compromised email account).
- Compare the compromised system to a known good copy.
- Anomaly detection/behavior monitoring (compare to preestablished baseline).

Key Decisions for Exiting Containment and Investigation Phase

- The attacker's ability to affect the network has been effectively controlled/stopped.
- The affected system(s) are identified.
- Compromised systems volatile data collected, memory image collected, and disks are imaged for analysis.
- Investigation of Root Cause has been conducted or, at a minimum, begun.

Examples of when to return to the Containment and Investigation Phase:

- Additional attacker activity is found beyond the scope of containment.
- Evidence of attacker activity is found that pre-dates the assumed initial point of compromise or root cause.
- The incident had to be reassessed and the scope could now be beyond initial containment strategies.

Phase IV – Eradication Details

The Eradication consists of full elimination of all components of the incident.

Eradication

NOTE: The specific administrative tools on a compromised host could be altered versions of the originals. Use a separate set of administrative tools (e.g. boot disk) than those on a compromised host for investigation whenever possible.

Steps to eradicate components of the incident may include:

- Disable breached user accounts.
- Reset any active sessions for breached accounts.
- Identify and mitigate vulnerabilities leveraged by the attacker.
- Close unnecessary open ports.
- Increase authentication security measures (implement MFA, add geolocation restrictions).
- Increase security logging, alerting, and monitoring.
- Clean installation of affected operating systems and applications.

All re-installed operating systems and applications must be installed according to Yellowstone County system build standards, including but not limited to:

A. Applying all the latest security patches.
B. Disabling all unnecessary services.
C. Installing anti-virus software.
D. Applying Yellowstone County hardened system configuration baselines.
E. Changing all account passwords (including domain, user and service accounts).

NOTE: It may be possible to restore the system without the need to perform a full clean installation. IT personnel, at the direction of the CSIRT, will make this determination.

Key Decisions for Exiting Eradication Phase

- Has the root cause been identified and identified vulnerabilities been remediated?
- Have all impacted accounts, including CSIRT burner credentials been reset?
- CSIRT is confident that the network and systems are configured to eliminate a repeat occurrence.
- There is no evidence of repeat events or incidents.
- Sign-off from IR Commander for all incidents.
- Notify County Commissioners.

Examples of when to return to the Eradication Phase:

- Additional compromised components or artifacts are discovered left over after the Eradication Phase.

Phase V – Recovery Details

Prior to restoring systems to normal operation, it is critical that the CSIRT validate the system(s) to determine that eradication was successful, and the network is secure. Once the organization has been attacked successfully, the same attackers will often attack again using the same tools and techniques leveraged in the initial attack. Having gained access to the compromised system(s) or network once, the attacker has more information at their disposal to leverage in future attacks.

If feasible, the system should be installed in a test environment to determine functionality prior to re-introduction into a production environment.

Furthermore, network monitoring should be implemented for as long as necessary to detect any unauthorized access attempts.

Recovery steps may include:

- Restoring systems from a clean backup.
- Replacing corrupted data from a clean backup.
- Restoring network connections and access rules.
- Communicating with interested parties about changes related to increased security.
- Increasing network and system monitoring activities (short or long-term).
- Increasing internal communication/reporting related to monitoring.
- Engaging a third party for support in detecting or preventing future attacks.

Key Decisions for Exiting Recovery Phase

- Business systems, services, and operations been restored to pre-incident or new-normal levels.

Examples of when to return to the Recovery Phase:

- Business systems, services, or operations are found to still be unacceptably degraded following incident response activities.

Phase VI - Lessons Learned

The follow-up phase includes reporting and post-incident analysis on the system(s) that were the target of the incident and other potentially vulnerable systems. The objective of this phase is continued improvement to applicable security operations, response capabilities, and procedures.

Documentation

All details related to the incident response process must be formally documented and filed for easy reference. The following items must be maintained, whenever possible:

A. All system events (audit records, logs).
B. All actions taken (including the date and time that an action is performed).
C. All external conversations.
D. Investigator Notes compiled.
E. Any deviations from SOP and justifications.

An incident report, documenting the following will be written by the CSIRT at the end of the response exercise:

A. A description of the exact sequence of events.
B. The method of discovery.
C. Preventative measures put in place.
D. Assessment to determine whether recovery was sufficient and what other recommendations should be considered.

The objective of the report is to identify potential areas of improvement in the incident handling and reporting procedures. Hence, the review of the report by management should be documented, together with the lessons learned, to improve on the identified areas and used as reference for future incidents.

Lessons Learned and Remediation

The CSIRT will meet with relevant parties (technical staff, management, vendors, security team, etc.) to discuss and incorporate lessons learned from the incident to mitigate the risk of future incidents. Based on understanding of the root cause, steps will be taken to strengthen and improve Yellowstone County information systems, policies, procedures, safeguards, and/or training as necessary. Where mitigations or proposed changes are rejected, a Risk Acceptance Process must be followed. Incidents should be analyzed to look for trends and corrective action should be considered where appropriate.

Lessons Learned discussion should cover:

- Review of discovery and handling of incident(s).
- How well staff and management performed and whether documented procedures were followed.
- Review of actions that slowed or hindered recovery efforts.
- Proposed improvements to future response and communication efforts.

- Recommendations to increase the speed of future detection and response efforts.
- Recommendations for long and short-term remediation efforts.

At the end of Lessons Learned meetings, some sort of remediation needs to occur, either resolving the issues, installing compensating controls, or at a minimum formally assessing and accepting the risk. Recommendations for long and short-term remediation efforts must be added into the overall treatment plan.

Updates to the incident response procedures should also be considered and incorporated where areas of improvement are found.

Voluntary information sharing should occur whenever possible with external stakeholders to achieve broader cybersecurity situational awareness (InfraGard, ISAC, etc.). Legal and Management must be consulted before doing so if a formal Information Sharing policy and process do not exist.

Forensic Analysis & Data Retention

In the event of possible legal action, forensic analysis will ensue in such manner as to preserve digital evidence consistent with legislative and legal requirements. Outside legal counsel and forensic experts may be required.

Consider the following when deciding whether and for how long to retain evidence related to the incident:

- Prosecution – is it likely that the attacker will be prosecuted? If so, evidence may need to be retained for multiple years.
- Reoccurrence – consider whether the evidence collected may be useful in case the attacker or a similar attack should occur in the future.
- Data Retention Policies – Consider the contents of evidence held (such as a system image capture) and retention policies related to this data (e.g. email retention policy).
- General Records Schedule (GRS) 24 specifies that incident handling records should be kept for three years.
- Cost – Depending on the type and amount of data or equipment preserved as evidence, cost may be a limiting factor.

Key Decisions for Exiting Lessons Learned Phase

- Management is satisfied that the incident is closed.
    - IR Commander makes the decision for limited-severity incidents. County Commissioners makes the decision for moderate and critical-severity incidents.
- There is an action plan to respond to operational issues which arose from this incident.

- Include schedules and accountability for completion of action plan items.
- At this point, it is time to return to the Preparation Phase (See Figure 1:PICERL Framework Model).

Examples of when to return to the Lessons Learned Phase:

- If items on the action plan are found to be incompletable or solutions are later deemed unreasonable. New solutions will need to be identified and the action plan updated.

Plan Testing and Review

The Yellowstone County Incident Response Plan and procedures must be tested at least annually. The IR Commander will conduct training using a scheduled simulated incident to guide and test procedures. (Refer to *NIST SP 800-61r2, Appendix A—Incident Handling Scenarios* for test scenarios) The plan and procedures will be updated to reflect lessons learned and to incorporate any new industry developments.

CSIRT members and the IT Director must participate in test exercises at least annually.

The Incident Response Plan and procedures are reviewed no less than annually and updates are tracked in the version history on page 1.

Plan review should include:

- Review supporting documents and forms listed in the Supporting Document List(Appendix IX) to ensure they are accurate and effective.
- Review Appendices to ensure they are accurate and effective.
- Review completed Incident Reporting Forms and corrective action plans for recommended plan and procedure updates.
- Compare recent changes to the organization's infrastructure and management structure to documented plan and procedures.

Appendices

Index of Appendices

Appendix I. Logging, Alerting, and Monitoring Activities List

Logging, alerting, and monitoring activities may target individual systems or a range of activities across multiple systems and applications. Keep a list of logging, alerting, and monitoring activities and review the list regularly to ensure that technicians can respond to abnormal events quickly. If you have a managed asset inventory these activities may be added to the existing list.

Prepared by:	**Jim Nelson; Steve Y.**			**Date updated:**	4/23/25
System/Application Name	**Logging System**	**Events Logged**	**System Owner**	**Monitoring frequency**	**Alerting**
M365 (exchange and Teams)	Cloud	Authentication, configuration changes, service startup/shutdown/restart	Laura Grieshop	when alerts are received	Automated email
Virtual Server Environment	Local	Content changes, administrator authentication	Konnie Rutherford	When alerts are received	Security and performance email
Kiwi syslog server	Local	Non-firepower firewall logs and some core network distributing logs	Konnie Rutherford	Triggered from other system alerts	None
Fire-power logs: Pointing to the FMC V-Environment	Local	Fire-power logs	Konnie Rutherford / Jenna Masters	Informal but reviewing consistently	Critical Alerts
KnowBe4	Cloud	Suspicious phishing emails	Jenna Masters – Network Admin	Daily monitoring	User alerts
Cisco IronPort	Cloud	Suspicious email triggers	Konnie Rutherford / Jenna Masters	Informal but reviewing consistently	Minimal (email bounces, etc.)
SentinelOne/Endpoints	Cloud	Winevent logs	Konnie Rutherford / Will Grimm	Eventviewer logs are captured on a 2 week basis	Standard alerting
Web Application Firewall	Local; DMZ	Activity, access to public websites	Jamie DeBree	Daily	Critical alerts – email

Appendix II. Two-Minute Incident Assessment Reference

Step 1: Understand impact/potential impact. (and likelihood if not an active incident)

- What is the value of the asset? If not significant, why react?
- Roughly quantify the potential worst-case impact.
- Include rough estimate of likelihood of experiencing this impact.

Step 2: Identify suspected/potential cause(s) of the issue.

- Any and all possible scenarios should be considered.
- Quickly eliminate those that can be proven incorrect.
- Share most likely scenarios when communicating.

Step 3: Describe recommended containment and remediation activities.

- How do you close the hole/stop the bleeding?
- Include any steps that could reduce the experienced impact.
- Don't forget about reputation damage and legal expectations.

Step 4: Communicate to Management.

- Describe the issue at a high level. (what and how it happened)
- Explain what it means to the business. (financial, reputation, etc.)
- Share short-term actions needed to move the risk from critical/high to something more acceptable.

Two-Minute Incident Assessment Form

Replace the example in the second column with known information about the (potential) incident.

Step 1: Impact/potential impact (and likelihood)	
Value of the Asset (H/M/L)	Example of high might be access to the full client database vs. low might be a proprietary internal process document with limited IP.
Potential Impact	What would the loss or felt impact be if the incident were real and fully realized? Try to quantify into both $ and impact like reputation or legal liability.
Likelihood of Impact	Immediate risk (internet accessible cataloged trivial vulnerability to exploit) of not likely known and complex (requires sophisticated expertise and specific circumstances to exploit)
Step 2: Suspected/potential cause(s) of the issue	
Suspected causes (list all potential causes that should be investigated)	Configuration error, remote vulnerability exploited, lost device, targeted denial of service by political or financially motivated party (DDOS to cover up a fraud), etc.
(Pause and quickly eliminate possible scenarios that can be proven incorrect.)	
Most likely cause(s)	These sources should be quickly pursued to prove correct or incorrect.
Step 3: Describe recommended containment and remediation activities	
Recommended containment	Stop the bleeding. Turn off internet, remove server from external access, disable account, remote wipe a device, etc.
Recommended steps to reduce impact	Notify management and legal teams, communicate issue to employees or customers
Recommended remediation (fix)	Implement a patch or configuration change, reset user credentials, deploy multi-factor, etc.
Step 4: Communicate to Management	
Describe issue in simple terms	Describe the problem within a business context if possible. Examples are useful to illustrate the issue in operational terms.
Explain the "So What" factor	Why is this important to our business? What could it cost us if we fail to act?
Suggested Immediate Actions	Propose specific responses and why we should take them. What will taking that action provide the business with regards to reduced impact or liability? There may be more than one potential path. If there are viable options, they should be presented for decisioning.
Other Proposed Remediation	Are there follow-on risks that require additional action? Examples are communication strategy, user awareness activities, process changes, systems/tools enhancements or implementations (long-term actions)

Appendix III. Incident Response Checklist

Refer to the Incident Response Form in (Location).

No.	Description	Remarks
	Preparation Phase (IR Commander)	
1	Prepare contact list and disseminate to relevant parties	
	Identification (IT Support)	
2	Complete sections 1 and 2 of the Incident Response Form	
	Assessment (CSIRT)	
3	Complete sections 3 – 5 of the Incident Response Form	
4	Notify relevant parties.	
	Containment (CSIRT/Support)	
5	Perform system backup to maintain current state of the system	
6	Change local passwords for the affected system(s)	
	Eradication (CSIRT/Support)	
7	Do not use the system administrative tools. Use separate administrative tool sets for investigation.	
8	Re-install a clean operating system	
9	Harden the operating system (e.g. apply patches, disable unnecessary services, install anti-virus software, etc.)	
	Recovery (CSIRT/Support)	
10	Validate that the system has been hardened	
11	Restore system data with clean backup	
12	Put the affected system(s) under network surveillance for future unauthorized attempts	
	Follow-up (IR Commander)	
13	Perform post-mortem analysis on affected system(s) to identify (potential) vulnerable areas	
14	Submit an Incident Response Report for management review	
15	File all documentation on the incident response process for future reference	

Appendix IV. Notification Requirements

List all requirements that apply to the organization

Requirement	Clients Impacted	Notification Timing	Notes
PCI DSS	County citizens who pay various fees/accounts with a credit card	Immediately, no later than 24 hours after discovery	
HIPAA	Youth Services Center Customer Personal Health Information (PHI)	No later than 60 days following a breach	
State of MT		Immediately, but may be delayed at law enforcement advisement	

PCI DSS

Any security incident involving a breach of cardholder data must adhere to all notification and response requirements of the Payment Card Industry (PCI) Security Standards Council.

Visa

Taking immediate action

Merchants and service providers that have experienced a suspected or confirmed security breach must take immediate action to help prevent additional damage and adhere to Visa CISP requirements.

Alert all necessary parties immediately:

- Your internal incident response team and information security group.
- Your merchant banks.
- If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Commander immediately at U.S. – (650) 432-2978 or usfraudcontrol@visa.com

Loss or theft of account information

Members, service providers or merchants must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data.

Forensic Investigation Guidelines

A Visa client/member or compromised entity must engage a Payment Card Industry Forensic Investigator (PFI) to perform a forensic investigation. Visa will NOT accept forensic reports from non-approved forensic companies. It is the Visa client or member's responsibility to ensure their merchant or agent engage a PFI to perform a PFI forensic investigation. Visa has the right to engage a PFI to perform a further forensic investigation as it deems appropriate and will assess all investigative costs to the appropriate Visa client, in addition to any assessment that may be applicable. PFIs are required to release forensic reports and findings to Visa. All PFIs must utilize Payment Card Industry reporting templates.

Note: For a list of PFIs, please go to: https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php.

Note: Visa has the right to reject the report if it does not meet the PFI requirements. PFIs are required to address with Visa, the acquirer, and the compromised entity, any discrepancies before finalizing the report.

To preserve evidence and facilitate the investigation:

- Do not access or alter compromised system(s) (e.g., don't log on at all to the compromised system(s) and change passwords; do not log in as ROOT). Visa highly recommends the compromised system not be used to avoid losing critical volatile data.
- Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (e.g., unplug network cable, shut down switchport, etc.).
- Preserve all evidence and logs (e.g., original evidence, security events, web, database, and firewall logs, etc.)
- Document all actions taken, including dates and individuals involved.
- If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
- Block suspicious IPs from inbound and outbound traffic.
- Be on high alert and monitor traffic on all systems with cardholder data.

For more information on the forensic investigation guideline, please refer to the document labeled PCI Forensic Investigator (PFI) Program Guide.

MasterCard

The MasterCard Account Data Compromise User Guide sets forth instructions for MasterCard members, merchants, and agents, including but not limited to member service providers and data storage entities

regarding processes and procedures relating to the administration of the MasterCard Account Data Compromise (ADC) program.

Discover

To contact Discover regarding Data Security or PCI Compliance:

Data Security: 1-800-347-3083 Call Mon–Fri 8:30am to 12:30pm and 1:30pm to 4:00pm Eastern Time, excluding holidays.

Questions on Security or PCI Compliance: AskDataSecurity@discover.com

Report data compromise or cardholder data breach: 1-800-347-3083 Call Mon–Fri 8:30am to 4:00pm Eastern Time, excluding holidays.

American Express

Data Incident response Obligations: Merchants must notify American Express immediately and in no case later than twenty-four (24) hours after discovery of a Data Incident.

To notify American Express, please contact the American Express Enterprise Incident Response Program (EIRP) toll free at (888) 732-3750 (US only), or at 1-(602) 537-3021 (International), or email at EIRP@aexp.com. Merchants must designate an individual as their contact regarding such Data Incident.

Please see the American Express Data Security Operating Policy for all details pertaining to Data Incident response Obligations.

HIPAA

Reference: http://www.hhs.gov/hipaa/for-professionals/breach-notification/

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

HIPAA Breach Definition

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

There are three exceptions to the definition of "breach."

- The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
- The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

If a covered entity determines that a breach has occurred, the following breach notification obligations apply:

1. **Notice to Individuals:** Affected individuals must be notified without unreasonable delay, but in no case later than 60 calendar days after discovery.
    a. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
2. **Notice to Media:** If a breach affects more than 500 residents of a state or smaller jurisdiction, the covered entity must also notify a prominent media outlet that is appropriate for the size of the location with affected individuals.

3. **Notice to HHS:** Information regarding breaches involving 500 or more individuals (regardless of location) must be submitted to HHS without reasonable delay and no later than 60 days following a breach.
    a. If a particular breach involves 500 or fewer individuals, the covered entity is required to report the breach to HHS within 60 days after the end of the calendar year in which the breach occurred via the HHS web portal.
4. **Notice by Business Associates to Covered Entities:** A business associate of a covered entity must notify the covered entity if the business associate discovers a breach of unsecured PHI. Notice must be provided without unreasonable delay and in no case later than 60 days after discovery of the breach. See the **Customer Data Breach Report** (location).
5. **Administrative Requirements and Burden of Proof:** Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of “breach.”

State of Montana

For a listing of all states, see this link: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Definitions

2-6-1501. Definitions. As used in this part, the following definitions apply:

(1) "Breach of the security of a data system" or "breach" means the unauthorized acquisition of computerized data that:

(a) materially compromises the security, confidentiality, or integrity of the personal information maintained by a state agency or by a third party on behalf of a state agency; and

(b) causes or is reasonably believed to cause loss or injury to a person.

(2) "Chief information security officer" means an employee at the department of administration designated by the chief information officer who is responsible for protecting the state's information assets and citizens' data by:

(a) advising and overseeing information security strategy and programs for executive branch state agencies without elected officials;

(b) advising and consulting information security strategy and programs for executive branch state agencies with elected officials and the legislative and judicial branches; and

(c) advising information security strategy and programs for city, county, consolidated city-county, and local governments and for school districts, other political subdivisions, or tribal governments.

(3) "Individual" means a human being.

(4) "Person" means an individual, a partnership, a corporation, an association, or a public organization of any character.

(5) (a) "Personal information" means a first name or first initial and last name in combination with any one or more of the following data elements when the name and data elements are not encrypted:

(i) a social security number;

(ii) a driver's license number, an identification card number issued pursuant to **61-12-501**, a tribal identification number or enrollment number, or a similar identification number issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands, or American Samoa;

(iii) an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account;

(iv) medical record information as defined in **33-19-104**;

(v) a taxpayer identification number; or

(vi) an identity protection personal identification number issued by the United States internal revenue service.

(b) The term does not include publicly available information from federal, state, local, or tribal government records.

(6) "Redaction" means the alteration of personal information contained within data to make all or a significant part of the data unreadable. The term includes truncation, which means that no more than the last four digits of an identification number are accessible as part of the data.

(7) "Security incident" means an occurrence that:

(a) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or

(b) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(8) (a) "State agency" means an agency, authority, board, bureau, college, commission, committee, council, department, hospital, institution, office, university, or other instrumentality of the legislative or executive branch of state government. The term includes an employee of a state agency acting within the course and scope of employment.

(b) The term does not include an entity of the judicial branch.

(9) "Third party" means:

(a) a person with a contractual obligation to perform a function for a state agency; or

(b) a state agency with a contractual or other obligation to perform a function for another state agency.

Protection Of Personal Information -- Compliance -- Extensions

2-6-1502. Protection of personal information -- compliance -- extensions. (1) Each state agency that maintains the personal information of an individual shall develop procedures to protect the personal information while enabling the state agency to use the personal information as necessary for the performance of its duties under federal or state law.

(2) The procedures must include measures to:

(a) eliminate the unnecessary use of personal information;

(b) identify the person or state agency authorized to have access to personal information;

(c) restrict access to personal information by unauthorized persons or state agencies;

(d) identify circumstances in which redaction of personal information is appropriate;

(e) dispose of documents that contain personal information in a manner consistent with other record retention requirements applicable to the state agency;

(f) eliminate the unnecessary storage of personal information on portable devices; and

(g) protect data containing personal information if that data is on a portable device.

(3) Except as provided in subsection (4), each state agency that is created after October 1, 2015, shall complete the requirements of this section within 1 year of its creation.

(4) The chief information officer provided for in **2-17-511** may grant an extension to any state agency subject to the provisions of the Montana Information Technology Act provided for in Title 2, chapter 17, part 5. The chief information officer shall inform the governor, the office of budget and program planning, and the legislative finance committee of all extensions that are granted and of the rationale for granting the extensions. The chief information officer shall maintain written documentation that identifies the terms and conditions of each extension and the rationale for the extension.

Notification Of Breach Of Security Of Data System

2-6-1503. Notification of breach of security of data system. (1) (a) Upon discovery or notification of a breach of the security of a data system, a state agency that maintains computerized data containing personal information in the data system shall make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

(b) The notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (3) or with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

(2) (a) A third party that receives personal information from a state agency and maintains that information in a computerized data system to perform a state agency function shall:

(i) notify the state agency immediately following discovery of the breach if the personal information is reasonably believed to have been acquired by an unauthorized person; and

(ii) make reasonable efforts upon discovery or notification of a breach to notify any person whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person as part of the breach. This notification must be provided in the same manner as the notification required in subsection (1).

(b) A state agency notified of a breach by a third party has no independent duty to provide notification of the breach if the third party has provided notification of the breach in the manner required by subsection (2)(a) but shall provide notification if the third party fails to do so in a reasonable time and may recover from the third party its reasonable costs for providing the notice.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay of notification. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation.

(4) All state agencies and third parties to whom personal information is disclosed by a state agency shall develop and maintain:

(a) an information security policy designed to safeguard personal information; and

(b) breach notification procedures that provide reasonable notice to individuals as provided in subsections (1) and (2).

(5) A state agency or third party that is required to issue a notification to an individual pursuant to this section shall simultaneously submit to the state's chief information security officer at the department of administration and to the attorney general's consumer protection office an electronic copy of the notification and a statement providing the date and method of distribution of the notification. The electronic copy and statement of notification must exclude any information that identifies the person who is entitled to receive notification. If notification is made to more than one person, a single copy of the notification that includes the number of people who were notified must be submitted to the chief information officer and the consumer protection office.

Immediate Notification

2-6-1504. Immediate notification. On discovery or notification of a security incident, a state agency shall provide immediate notification without unreasonable delay to the chief information security officer.

Appendix V. Media Statements

Below are sample statements to use if members of the media call before a press release is issued. ***All communications with the media should be directed to the Incident Response Commander or other representative designated by executive management.*** Getting the facts correct is a priority. Do not give information to the media before confirming facts with internal personnel and management. Changing information after it is released can lead to media confusion and loss of focus on the key messages.

Pre-scripted Immediate Responses to Media Inquiries

Use this template if the media is "at your door" and you need time to assemble the facts for the initial press release statement.

Getting the facts is a priority. It is important that Yellowstone County not give in to pressure to confirm or release information before you have confirmation.

The following responses give you the necessary time to collect the facts.

Pre-scripted Responses

If on the phone to the media:

- "We've just learned about the [situation, incident, event] and are trying to get more complete information now. How can I reach you when I have more information?"
- "All our efforts are directed at [bringing the situation under control]. I'm not going to speculate about [the situation]. How can I reach you when I have more information?"
- "I'm not the authority on this subject. Let me have [name] call you right back."
- "We're preparing a statement now. Can I get back to you in about [number of minutes or hours]?"
- "You may check our website for background information, and I will fax/e-mail you with the time of our next update."

If in person at the incident site or in front of a press meeting:

- This is an evolving [situation, incident, event], and I know you want as much information as possible right now. While we work to get your questions answered, I want to tell you what we can confirm right now:
- At approximately [time], a [brief description of what happened].
- At this point, we do not know [how long the advisory will last, how many customers are affected, etc.].
- We have a [system, plan, procedure, operation] in place. We are being assisted by [local officials, experts, our legal team] as part of that plan.

- The situation is [under, not yet under] control. We are working with [local, state, federal] authorities to [correct this situation, determine how this happened].
- We will continue to gather information and release it to you as soon as possible. I will be back to you within [amount of time in minutes or hours] to give you an update. As soon as we have confirmed information, it will be provided.
- We ask for your patience as we respond to this [situation, incident, event].

Statement Writing Tips

The following information/tips can be used to create a good media statement. Not all of them need to be included, but typically two or three will ensure an effective statement.

Honesty

If Yellowstone County is at fault, admit it. By attempting to deflect responsibility, journalists and the public will be far less forgiving when the details around the incident are exposed, and the County is found wanting. Even in a real crisis, you can gain respect for holding your hands up.

If it is not your fault, you need to make it very clear without overtly blaming any other individual or organization.

- Words to use: take or share responsibility, committed to openness, transparent.
- Words not to use: blame, fault.

Context

Presenting negatives in a broad context can go a long way to minimizing the impact of the bad news.

If the story is about a service user who has had a bad experience, you can refer to the many other service users who have had good experiences. This is where external advocates are useful – particularly other service users.

Broadening context also means isolating the incident – simply a case of stating that the negative incident is 'very rare'/'isolated' and placing it within a wider, more positive framework.

- Words to use: very rare, isolated.
- Words not to use: frequent mistakes, another error.

Framing Effect

The Framing Effect is a form of cognitive bias, which causes people to prefer positive sounding statements over negative ones, despite otherwise being logically identical. For example, when discussing a risky surgery, patients will be a lot more likely to go through with a surgery when it is explained that "the odds of survival one month after surgery is 90%" as opposed to "mortality within

one month of surgery is 10%" despite both statements equating to the same amount of risk. Be aware of this form of cognitive bias when developing and delivering messages to the public.

Partnership

There are occasions when it is useful to subtly remind a critical audience that you are not solely responsible for the conduct of a particular individual. This can be achieved without it appearing as if you are 'buck-passing' or absolving yourselves of responsibility and without upsetting relations with other key partners.

For example, you may simply state that 'as one of a number of organizations involved in supporting the individual concerned, you are 'committed to providing the best possible service for service users in the area'.

- Word to use: working together; joint responsibility, as one of a number of organizations.
- Words not to use: X is to blame; we don't know what others think of this but.

Action

Media statements should not merely talk about the problem; they should stress action on the part of the organization.

You will not improve any media situation if you are seen to be passive in the case of a negative situation or media crisis.

A word of caution: avoid saying you will be holding an 'investigation'/'inquiry' in the case. These words are headline fodder for the media and can imply guilt.

- Words to use: taking immediate action, taking appropriate measures, working closely with.
- Words not to use: we are holding an investigation; we will look into it.

Positives

Don't be afraid to point out how successful your organization is in any media statement. Mistakes happen and emphasizing the positive things you've done can help people see past minor blips.

- Words to use: we have seen positive results, we have been successful in, we will continue to provide the best service.
- Words not to use: there are a number of areas we need to work on (unless you accompany that with a positive statement, e.g., that you will be taking measures to change this).

Empathy

Negative media situations obviously create a gap between you and the public involved. Expressions of empathy can help bridge the gap.

- Words to use: we understand, we appreciate, we know, we recognize.
- Words not to use: these things happen, everyone faces these issues.

Be Concise

Journalists are typically not interested in lengthy statements – they would prefer to spend the effort on details of the event/incident. Further, if the person speaking with the media is not accustomed to doing so, lengthy statements may result in the speaker making an error.

As a rule, statements for printed media should be no more than two paragraphs long – one tight sentence per paragraph.

Broadcast media may give you more space, but you should still bear length in mind as the producer/editor may be looking to produce a shortened version of your statement to drop into a later news bulletin.

Statements Should Avoid

- **Confrontation** - the objective of media statements in a crisis is to diffuse the situation – not make it worse. Avoid blaming/buck-passing because it will simply result in a media-based argument between opposing parties – remember journalists love confrontational stories. e.g., 'They were wrong', 'it is not our fault'…
- **Ambiguity** - weak, ambiguous statements have no place in handling negative media situations and can leave room for the journalist to re-interpret your response. Be robust and clear at all times. Use strong positive words, e.g., 'we are committed to X and will not tolerate Y'. Make sure your statement is completely unambiguous.
- **Personal pronouns** - try and avoid referring to your organization by name in your media statement as doing this could reinforce the link between your organization and the negative issue concerned. You may simply use the first-person plural ('we'/'us'). This also has the advantage of adding a slightly personal and less bureaucratic feel to the statement.

Appendix VI. Customer Letter Template

Formal Email and/or Letter Template

Dear Valued Customer,

As you may be aware, Yellowstone County has announced that it experienced a criminal intrusion into a portion of its computer network in some of its retail stores. This criminal intrusion may have resulted in the theft of account numbers, expiration dates, and other numerical information and/or the cardholder's name. The company has not determined that any such cardholder data was in fact stolen by the intruder, and it has no evidence of any misuse of such data.

Yellowstone County is providing this notice out of an abundance of caution to all of its customers who have provided their contact information to the company, including you. **YOUR INFORMATION IS NOT NECESSARILY AFFECTED**.

Yellowstone County believes that the potentially impacted systems were breached during the period of <insert date> through <insert date>.

Upon recognition of the intrusion, Yellowstone County took immediate steps to secure the affected part of its network. An investigation supported by third-party data forensics experts is going on to understand the nature and scope of the incident. Yellowstone County believes the intrusion has been contained and is confident that its customers can safely use their credit and debit cards in its stores. Yellowstone County currently has no reason to believe that additional information beyond that described above was stolen by the intruder. However, given the continuing nature of this investigation, it is possible that time frames, location, and/or at-risk data in addition to those described above will be identified in the future.

The Company has notified federal law enforcement authorities and is cooperating in their efforts to investigate this intrusion and identify those responsible for the intrusion. The press release and this letter have not been delayed as a result of this law enforcement investigation. Yellowstone County has also notified the major payment card brands and is cooperating in their investigation of the intrusion.

Yellowstone County has established a call center to answer customer questions about the intrusion and the identity protection services being offered. The call center will be staffed Monday through Friday 8am-8pm CST.

You are a valued customer, and we regret any inconvenience that this may cause you.

Sincerely,

<insert name and title>

Possible other considerations to include depending on the nature of the incident.

- Provide free credit reports (www.annualcreditreport.com or 1-877-322-8228)
- Fraud Alerts – Equifax (www.equifax.com or 1-877-478-7625), Experian (www.experian.com or 1-888-397-3742), TransUnion Fraud Victim Assistance Division (www.transunion.com or 1-800-680-7289)

Appendix VII. Incident Response Organizations

Below is a list of incident response organizations that may be useful in planning for or responding to an incident:

Organization	URL
Anti-Phishing Working Group (APWG)	https://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), US Department of Justice	https://www.justice.gov/criminal-ccips
CERT Coordination Center	https://www.sei.cmu.edu/about/divisions/cert/index.cfm
European Network and Information Security Agency (ENISA)	https://www.enisa.europa.eu/
High Technology Crime Investigation Association (HTCIA)	https://htcia.org/
InfraGard	https://www.infragard.org/
Internet Store Center (ISC)	https://isc.sans.edu/
National Council of ISACs	https://www.nationalisacs.org/
United States Computer Emergency Response Team (US-CERT)	https://www.us-cert.gov/
FRSecure	https://frsecure.com/

Appendix VIII. Cyber Insurance and Third-Party Service Agreements

Where Cyber Insurance or Third-Party Services are involved, having a clear understanding of their incident response and detection services is essential. For example, many cyber insurance carriers require the organizations they cover to follow a pre-defined process. Examples of third-party service providers that may be involved in IR activities include insurance providers, internet service provider (ISP), cloud service provider (CSP), software vendors, or a multiservice provider (MSP).

The IT DIrector is responsible for reviewing all SLAs with service providers to ensure that responsibilities and expectations are defined in relation to incident response.

IR Commanders are responsible for understanding SLAs with service providers and knowing when the team should engage the service provider.

Table 2: Third Party Support and Response

Service Provider	Applications/Services	When to contact	Service Level/Response Time
FRSecure	Incident Response Digital Forensic Investigation	During suspected incident, ongoing incident, or post incident investigation	4 hour maximum
HighPoint Networks	SentinelOne	During suspected Incident	Immediate
Cerium	Network; Firewall	During suspected Incident	Immediate

Table 3: Insurance Coverage and Contact Information

Insurance Provider	Limits	Term Dates	When to contact	Contact Information
Travelers Insurace	$3,000,000 $50,000 Retention	Aug 22,2023 – July 1, 2024	Immediately, any financial or data loss	Travelers: 1-800-842-8496 MarshMcLennan: Caitlin Finnicum Caitlin.Finnicum@MarshMMA.com 406-238-1996

**Additional coverage sub-limits may apply per claim.*

TRAVELERS

Wrap+®

Declarations

Policy No. 107738453

This Policy consists of this Declarations and one or more Coverage Declarations and Coverage forms. It may also include one or more Common Conditions or endorsements. In consideration of the premium, the Insurer provides this Policy, which is the entire agreement between the Insurer and the Insured.

Insurer	Throughout this Policy, Insurer means **Travelers Casualty and Surety Company of America**, which is a capital stock company located in Hartford, Connecticut.
Named Insured	Throughout this Policy, Named Insured means: YELLOWSTONE COUNTY
Principal Address	ATTN: FINANCE 217 NORTH 27th ST. BILLINGS, MT 59101
Policy Period	Inception: August 22, 2023 Expiration: July 01, 2024 12:01 A.M. local time both dates at Principal Address.
Policy Premium	$56,389.00
Total	$56,389.00
Notices To The Insurer	Mail: Travelers Bond & Specialty Insurance Claim P.O. Box 2989 Hartford, CT 06104-2989 Overnight Mail: Travelers Bond & Specialty Insurance Claim One Tower Square, S202A Hartford, CT 06183 Email: BSIclaims@travelers.com Fax: 1-888-460-6622 For questions related to claim reporting or handling, please call 1-800-842-8496.
Producer Information	MARSH & MCLENNAN AGENCY PO BOX 30638 BILLINGS, MT 59107 Phone: 406-721-1000

Authorized officers of the Insurer:

President

Corporate Secretary

Countersigned By

AFE-15001 Rev. 06-20

Page 1 of 2

CyberRisk Declarations

Claims-Made: The Liability Insuring Agreements are provided on a Claims-Made basis, and cover only *Claims* first made during the *Policy Period*, or any applicable extended reporting period. Please read the Policy.

Defense Within Limits: The Limit available to pay settlements or judgments will be reduced, and may be completely exhausted, by *Defense Costs*, and any retention will be applied against *Defense Costs*.

A limit left blank for a coverage means that such coverage is not included. An entry for any other provision left blank means that such provision does not apply.

The Insurer has the duty to defend *Claims*.

CyberRisk Aggregate Limit: $3,000,000

Liability	Limit	Retention
Privacy and Security	$3,000,000	$50,000
Payment Card Costs	$3,000,000	Subject to Privacy and Security Retention
Media	$1,000,000	$50,000
Regulatory Proceedings	$3,000,000	$50,000

Breach Response	Limit	Retention
Privacy Breach Notification	1,000,000 impacted parties	impacted parties threshold 100
Computer and Legal Experts	$1,000,000 which is separate from the CyberRisk Aggregate Limit	
Betterment	$100,000	
Cyber Extortion	$3,000,000	$50,000
Data Restoration	$3,000,000	$50,000
Public Relations	$3,000,000	$50,000

Cyber Crime	Limit	Retention
Computer Fraud	$100,000	$5,000
Funds Transfer Fraud	$100,000	$5,000
Social Engineering Fraud	$100,000	$50,000
Telecom Fraud	$100,000	$50,000

Business Loss	Limit	Retention
Business Interruption	$3,000,000	
Dependent Business Interruption	$100,000	
Dependent Business Interruption - System Failure	$100,000	
Dependent Business Interruption - Outsource Provider	$100,000	
Dependent Business Interruption - Outsource Provider - System Failure	$100,000	
Reputation Harm	$250,000	$5,000
System Failure	$3,000,000	

Additional First Party Provisions

Accounting Costs Limit:	$25,000
Betterment Coparticipation:	50%
Period Of Restoration:	180 days
Period Of Indemnity:	30 days
Wait Period:	12 hours

Knowledge Date: September 26, 2022

P&P Date: September 26, 2022

Retro Date: N/A

Extended Reporting Period

Months	Percentage of Annualized Premium
12	75%

CYB-15001 Rev. 06-20

Page 2 of 2

Direct questions about insurance coverage limits to the Risk Manager. Notify the Risk Manager to activate the insurance plan.

Appendix IX. Supporting Document List

- Incident Response Playbooks - \\intranet\IT_IncidentResponse
- Incident Handling Log and Assessment Tool - \\intranet\IT_IncidentResponse

BOARD OF COUNTY COMMISSIONERS

YELLOWSTONE COUNTY, MONTANA

_____

Mark Morse, Chairman

_____

Michael J. Waters, Member

_____

Chris White, Member

Incident Response Initiation Playbook, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document Owner: Yellowstone County IT Department
Last Review Date: August 2025

Incident Response Initiation Playbook

Version History

Version	Date	Author	Reason/Comments
1.00	May 2024	Jim Nelson/FRSecure	Document Origination
1.00	April 2025	Jim Nelson/Steve Yogodzinski	Review and move to approve
1.01	August 2025	Larry Ziler	Review for final approval
1.02	September 2025	Larry Ziler	Revisions from County Departments:
1.03	October 2025	Larry Ziler	Approved for submission to BOCC

The Incident Response Initiation Playbook (IRIP) is a working document meant to provide core incident response components. The IRIP provides the organization with an abbreviated IR action plan for the team on the ground working an incident as well as the first step in creating an overall Incident Response Plan (IRP).

Key Overall Contact Information

Name	Title	Role	Contact Information	Escalation (1-3)*
Larry Ziler	Information Technology Director	IR Commander, CSIRT manager	lziler@yellowstonecountymt.gov 406-696-9810	**1**
Melisssa Williams	Chief Civil Attorney	Communications Lead	mwilliams@yellowstonecountymt.gov 406-256-2832	3
Steve Williams	In-House Counsel	Communications Assistance	swilliams@yellowstonecountymt.gov	3
FRSecure	3rd Party Support	Incident Response and Digital Forensic Investigation	CSRIT@FRSecure.com	3
Traveler's Insurance	3rd Party Support	Cyber Insurance	Travelers Claim: 800-842-8496	3

			Marsh McLennan: Caitlin Finnicum Caitlin.Finnicum@MarshMMA.com 406-238-1996	
Jen Jones	Finance Director	Cyber Insurance (Internal); Public Relations	jjones@yellowstonecountymt.gov	3

*Escalation level determines order in which notification should occur:

1. notify first, required on all incidents
2. required on all moderate or high-severity incidents
3. involve as needed

Cyber Security Incident Response Team (CSIRT)

The CSIRT is comprised of IT management and experienced personnel. The role of the CSIRT is to promptly handle an incident so that containment, investigation, and recovery can occur quickly. Where third-party services are leveraged, ensure they are engaged as necessary.

No.	CSIRT Member	Role
1.	Larry Ziler	IR Commander –406-696-9810
2.	Jenna Masters	Network Administrator – jmasters@yellowstonecountymt.gov 406-208-7534
3.	Konnie Rutherford	IT Senior Engineer 406-606-0396
4.	Will Grimm	IT Specialist – wgrimm@yellowstonecountymt.gov 406-998-4309
5.	Ken Twichel	Phone Systems - ktwichel@yellowstonecountymt.gov 406-208-1780
6.	Laura Grieshop	Systems Administrator - lgrieshop@yellowstonecountymt.gov 406-894-0291
7.	Jamie DeBree	Web and Database Administrator – jdebree@yellowstonecountymt.gov 406-256-2761

Recorder

The Incident Response Manager will assign a team member to begin formal documentation of the incident. All incidents must be logged in the **Incident Handling Log & Assessment Tool**. A record of all action taken to remediate the incident, including chain of custody records, and deviations from SOP must be included in the documentation.

Reporting Incidents

Effective ways for both internal and outside parties to report incidents is equally critical as sometimes users of Yellowstone County systems and information may be the first to observe a problem. Review the different types of incidents addressed in Phase II under ***Error! Reference source not found.*** and list or establish reporting methods for a variety of incident types.

Reporting Method	Available To	Incident Type	Anonymous	Response Time
Service Desk Plus: Trackable ticket generation – contact method via email or dedicated phone number to Help Desk team	Employees	All Incident Types	No	Immediate during office hours. Otherwise within 1 hour of open.
Larry Ziler 406-696-9810	Employees	Off-hours Incidents	No	Immediate
Helpdesk	Employees	Off-hours Incidents	No	Immediate

Isolation/Containment

Compromised systems should be **disconnected from the network** rather than powered off.

Powering off a compromised system could lead to loss of data, information or evidence required for a forensic investigation later.

ONLY power off the system if it cannot be disconnected from the wired and wireless networks completely.

Incident Functional and Informational Impact

Once the categorization and scope of an incident has been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate the course of action to be taken to provide a resolution; however, in all instances an incident report must be completed and reviewed by the Incident Response Commander. Functional and informational impacts are defined with initial response activity below:

Functional Impact	Definition	CSIRT Response
None	No effect to the organization's ability to provide all services to all users.	Create ticket and assign for remediation.
Limited	Minimal effect: the organization can still provide all critical services to all users but has lost efficiency.	Create ticket and assign for remediation, notify the County Commissioners.
Moderate	The organization has lost the ability to provide a critical service to a subset of system users.	Initiate full CSIRT, involve the County Commissioners
Critical	The organization is no longer able to provide some critical services to any user.	Initiate full CSIRT and County Commissioners. Consider activation of the Disaster Recovery Plan

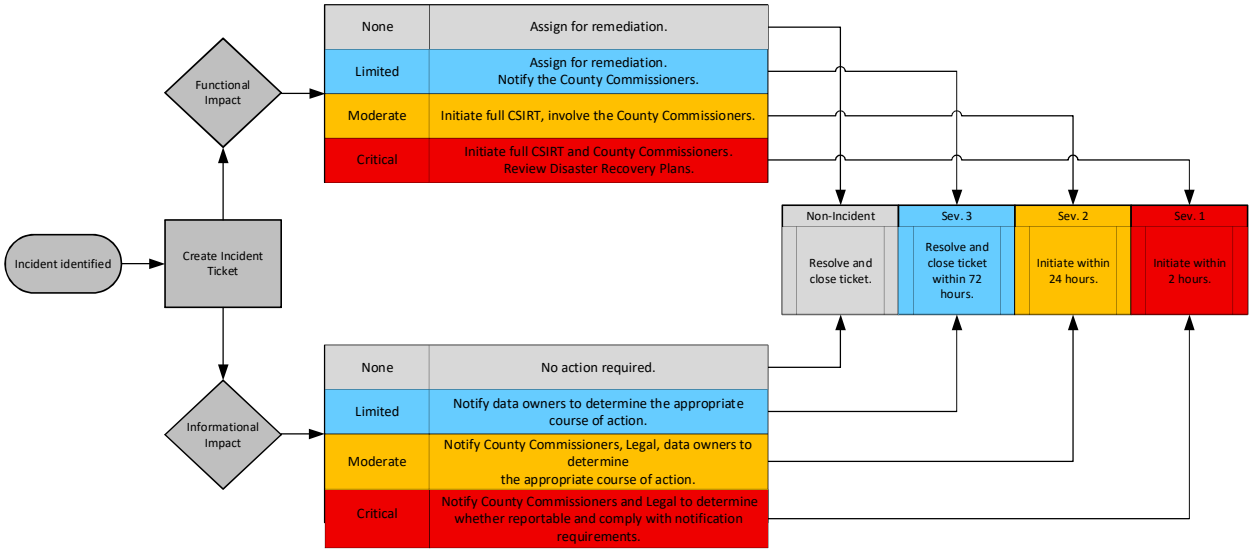
Informational Impact	Definition	CSIRT Response
None	No information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	No action required
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the data owners to determine the appropriate course of action.
Moderate	Internal Information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the County Commissioners. County Commissioners will work with management, legal, and data owners to determine appropriate course of action.
Critical	Protected Data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the County Commissioners. County Commissioners will work with legal to determine whether reportable, and the appropriate notification requirements.

The **Incident Handling Log & Assessment Tool** and Response Level table below will help determine the severity of the incident and urgency of response activities.

Response Level Classification		Informational Impact			
		None	Limited	Moderate	Critical
Functional Impact	None	N/A	Sev. 3	Sev. 2	Sev. 1
	Limited	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	Moderate	Sev. 2	Sev. 2	Sev. 2	Sev. 1
	Critical	Sev. 1	Sev. 1	Sev. 1	Sev. 1

The severity level should be used to determine how rapidly initial response activities should occur.

Severity Level	SLA
Sev. 3	Within three days
Sev. 2	Within 24 hours
Sev. 1	Within 2 hours



Key Decisions for Exiting Identification and Assessment Phase:

- If the Identification and Assessment process has determined the event constitutes a real incident, the IR process must be continued.
- All details in the Identification phase must be documented in the Incident Reporting Form if the event is determined to be an incident.

Engage Resources

The CSIRT should select the option based on the severity of the incident, the damage incurred by Yellowstone County and legal considerations.

	In-house investigation	Law enforcement	Private forensic specialist
Time Response	Quick response	Varies by area and agency	Quick response
Competency	Skills vary	Depends on local law enforcement	Highly skilled, often with law enforcement background
Preservation of evidence	Does not ensure evidence integrity	Preserve evidence integrity and present evidence in court	Preserve evidence integrity and present evidence in court
Reputation impact	Minimal effect	Potential loss of reputation if certain incidents reach public	Potential loss of reputation if certain incidents reach public

Incident Response Playbooks

- Business email compromise response playbook
- Credential theft response playbook
- Lost or stolen device response playbook
- Ransomware response playbook
- Web application compromise response playbook

Preserve Evidence

NOTE: If there is strong reason to believe that a criminal or civil proceeding is likely, the Yellowstone County Chain of Custody form must be used any time evidence has been taken into custody, or custody is transferred for the purpose of investigation.

Lessons Learned

The follow-up phase includes reporting and post-incident analysis on the system(s) that were the target of the incident and other potentially vulnerable systems. The objective of this phase is continued improvement to applicable security operations, response capabilities, and procedures.

Documentation

An incident report, documenting the following will be written by the CSIRT at the end of the response exercise:

A. A description of the exact sequence of events.

B. The method of discovery.
C. Preventative measures put in place.
D. Assessment to determine whether recovery was sufficient and what other recommendations should be considered.

The objective of the report is to identify potential areas of improvement in the incident handling and reporting procedures. Hence, the review of the report by management should be documented, together with the lessons learned, to improve on the identified areas and used as reference for future incidents.

Mitigation Discussions

The CSIRT will meet with relevant parties (technical staff, management, vendors, security team, etc.) to discuss and incorporate lessons learned from the incident to mitigate the risk of future incidents.

Lessons Learned discussion should cover:

- Review of discovery and handling of incident(s).
- How well staff and management performed and whether documented procedures were followed.
- Review of actions that slowed or hindered recovery efforts.
- Proposed improvements to future response and communication efforts.
- Recommendations to increase the speed of future detection and response efforts.
- Recommendations for long and short-term remediation efforts.

At the end of Lessons Learned meetings, some sort of remediation needs to occur, either resolving the issues, installing compensating controls, or at a minimum formally assessing and accepting the risk. Recommendations for long and short-term remediation efforts must be added into the overall treatment plan.

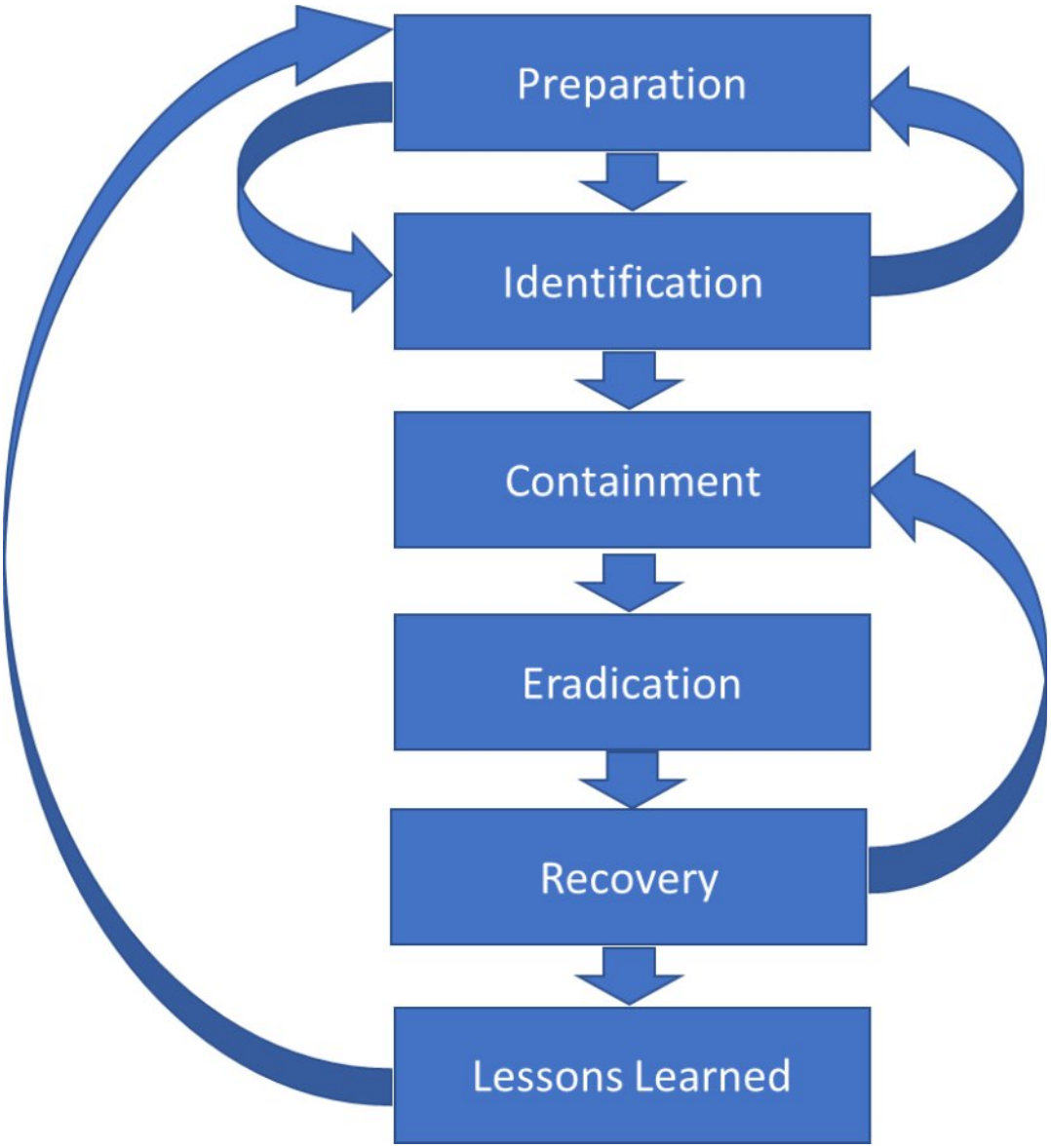


Figure 1:PICERL Framework Model

BOARD OF COUNTY COMMISSIONERS
YELLOWSTONE COUNTY, MONTANA

_____
Mark Morse, Chairman

_____
Michael J. Waters, Member

_____
Chris White, Member

B.O.C.C Thursday Discussion
Meeting Date: 10/23/2025
Title: CLOSED: STDF security
Submitted For: Melissa Williams, Deputy County Attorney
Submitted By: Melissa Williams, Deputy County Attorney

TOPIC:
CLOSED: STDF Security

BACKGROUND:
CLOSED: STDF security

RECOMMENDED ACTION:
Agenda Item
