[Insert Organization] Cybersecurity Incident Response Plan



[Remove and insert your organizations logo]

[CISA Cybersecurity Incident Response Plan for Small Organizations. Guidance, Templates and Playbooks (Version 2025-04)]

Version: 2025-07-14

Confidential

**Contents**

[Introduction 3](#_Toc190178892)

[Best Practices for CIRP 4](#_Toc190178893)

[Before a cybersecurity incident 4](#_Toc190178894)

[During a cybersecurity incident 6](#_Toc190178895)

[After a cybersecurity incident 7](#_Toc190178896)

[Cyber Incident Response Templates 8](#_Toc190178897)

[Executive Support, Responsibility, History, Change Log 9](#_Toc190178898)

[Incident Prioritization Impact levels 10](#_Toc190178899)

[Key Contacts 11](#_Toc190178901)

[Communication Channels to Notify Key Contacts and Stakeholders 13](#_Toc190178902)

[Essential Assets 14](#_Toc190178903)

[Essential Operational Technology (OT) Assets 16](#_Toc190178904)

[Simple Network Diagram 17](#_Toc190178905)

[Essential Software, Applications and Licensing 18](#_Toc190178906)

[Primary and Alternate Sites 19](#_Toc190178907)

[Asset Backup Information Details 20](#_Toc190178908)

[Incident Reporting Template 21](#_Toc190178909)

[Internal policies, laws, rules, regulations, and breach notification requirements 23](#_Toc190178910)

[Additional Incident Report Considerations and Questions 24](#_Toc190178911)

[Communication Templates 25](#_Toc190178912)

[Initial Incident Notification Template (Non-Public) 26](#_Toc190178913)

[Holding Statement Templates 27](#_Toc190178914)

[Public Information Release Template – Talking Points Guide 29](#_Toc190178915)

[Key Terms 30](#_Toc190178916)

[References 31](#_Toc190178917)

# Introduction

A Cyber Incident Response Plan (CIRP) is a written document, formally approved by the senior leadership team, that helps your organization before, during, and after a confirmed or suspected security incident. Your CIRP clarifies roles and responsibilities and provides guidance on key activities. It also includes a list of key people who may be needed during a crisis.

This CIRP template has been designed from several different resources which can be found on the last page of this document.

This document presents guidance, templates, playbooks, and best practices to quickly get started on your organization’s CIRP, or to enhance your existing CIRP. It is recommended that you review this document completely. Some of these templates and/or best practices may not be practical to implement for your organization. Use accordingly to create, modify, and/or add to your existing CIRP.

If you do not have an CIRP:

* Start by creating your first draft using the provided templates, completing the templates, and editing as necessary to meet your specific needs. Remove tables and rows in the templates that are not applicable to your organization.
* Once a draft is complete, share it with the appropriate staff to get their feedback and modify the plan accordingly.
* Once the draft CIRP is finalized, have it reviewed and ultimately approved by senior leadership.
* Following approval, it is recommended you print copies and store them in a location known to the CIRP Team who have a need to know.
* Train staff on the CIRP and location(s) of the hard copy and digital copies. Ensure that everyone is using the correct version!
* Identify and document possible areas for improvement.

If you already have an CIRP:

* Compare your CIRP with the provided templates and suggested “Best Practices.”
* Identify and document possible areas for improvement.

As you are creating or updating your CIRP, you might identify a best practice that isn’t documented in this resource. Please consider reaching out to your CISA Cybersecurity Advisor to discuss as it may be something to incorporate in future versions of this document and to share with other to help strengthen their CIRP.

The document was created for small sized organizations with little or no dedicated IT and/or Security staff or for those that use an IT Managed Service Provider. A similar mid to large organization template has been created for more detailed guidance and preparation activities. Contact your local CISA Cybersecurity Advisor for questions or additional resources.

# Best Practices for CIRP

## Before a cybersecurity incident

***Review the Incident Response plan at least annually***.

The best CIRPs are living documents that evolve with business changes. Consider creating a reoccurring appointment on a shared calendar to review and update the IR Plan. Consider a period each year where the office has more downtime for the review, for example the 1st week of December. Always ensure during the review that all staff are using and have access to latest version of the CIRP.

***Continuity Plan Activation Criteria***.

Ensure that the plan describes conditions that must be met before the plan can be executed.

***Train the staff at least annually***.

All staff need to understand their role(s) during incident. Discuss, define, and document procedures for each role. Consider scheduling the training once the plan has been reviewed and any changes that have been approved. Train by walking through the CIRP as a group. Identify who the *Incident Manager, Tech Manager and Communication Manager* will be, and who their backups are should they not be available. Backup roles should have authority and ability to make decisions should be primary be not available. Define in the plan when and how an incident is declared and by whom. Encourage staff to report possible cyber events to IT or the Managed Service Provider (examples: application or workstation is acting strange or abnormal, phishing email, social engineering call or email). Discuss how staff reports possible cyber events and when these events could become a possible incident (loss of critical service on all workstations, ransomware note(s), phishing email to multiple staff employees, etc.).

***Print the associated incident response plan providing a copy to everyone expected to play a role in an incident.***

During an incident, internal email, phones, chat, and document storage services may be unavailable or inaccessible. Print the incident response plan and put it in a designated secure location. Train staff on where it is located. Consider a specific-colored binder that Key Contacts can quickly identify. When the plan is updated, ensure the latest version is printed and put into binder. Ensure old version(s) are properly shredded or archived. Consider a secure online storage and offline storage for digital copies but have a plan to update all locations and communicate to appropriate staff when the plan has been modified or updated. It’s critical that everyone be using the same version of the CIRP.

***Define Roles – Incident Manager, Tech Manager, Communications Manager*.**

These roles should be defined, communicated, approved by leadership and users should be properly trained on these roles. Best practice is to define these roles prior to an incident, but they can also be assigned during an incident depending on Key Contacts and staff availability. These roles can be combined with another’s Job Title or Role. For example, the IT Contact may also be the Incident Manager and Tech Manager. Modify, redefine as necessary. Best practice is to only identify one individual for each of these roles. Should you define each role with a staff member prior to any incident, consider adding a backup or deputy for each in case the primary person is unavailable or until they arrive to take over from backup/deputy.

**Incident Manager (IM)**

This person leads the response. They manage communication flows, update stakeholders, and delegate tasks. However, the IM does not perform any technical duties. During a time of crisis, time dilation affects people’s perception of time passing. The IM will monitor the clock to avoid that common problem. The IM should also lead the hotwash meeting (outlined below) to gather lessons learned.

**Tech Manager (TM)**

This person serves as the technical subject matter expert. They will bring in other internal and possibly external technical experts (with the consent of the IM and possibly your attorney).

**Communications Manager (CM)**

The Communications Manager (CM) will interact with reporters, post updates on social media, and may interact with external stakeholders. This role is also sometimes referred as a Public Information Officer (PIO).

***Conduct a tabletop exercise (TTX) at least annually.***

Sometimes called an attack simulation exercise, a TTX is a role-playing game where a facilitator presents a scenario to the team. The exercise might start with the head of communications receiving an email from a reporter about rumors of a hack. The facilitator will provide other updates during the game to see how everyone plays their role. Every sports team rehearses, and you should too! [CISA can conduct TTXs](https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages) for you or you can use tabletop exercise packages to tailor and develop your own.

***Prepare press responses in advance.***

For example, should a reporter call your office claiming to know of data stolen from your fileservers, what will you say? Should you be saying anything at all? What about your staff? Who is the Communications Manager or Public Information Officer? If it’s you, having a good “holding statement” will help. Review the Communication Templates found within this guide for ideas.

***Select an outside technical resource/firm that will investigate/mitigate potential compromises***.

Consider this in the event you need physical, hands-on keyboards quickly. If this is not your IT or MSP – add this technical resource to your key contacts list.

***Establish a communications strategy***.

Document which communications channels will be used to notify stakeholders and Incident Management Key Contacts. This includes where to physically meet should communications be impacted or disabled. What are the alternate and approved ways to communicate (example: email, telephone/cellphone/radio, webinar meeting applications like Microsoft Teams, Google Meet, or Zoom). Emergency managers and local law enforcement may have some good ideas you can use. Consider talking with your Sheriff’s Office about 2-way radio backup communications. Incident Manager, Tech Manager and Communications Manager should work with IT to build email groups or appropriate meeting channels for quick alerting, online meetings and updating.

***Know how your critical information assets are backed-up and how long they are retained.***

Per [CISA/MS-ISAC #StopRansomware Guide](https://www.cisa.gov/resources-tools/resources/stopransomware-guide)***,*** it is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.

***Review your plan with your attorney, emergency manager*, *local law enforcement agency (LEA), and other important partners*.**

Your attorney and emergency manager may instruct you to use a completely different CIRP template. Attorneys often have preferences on how to engage with outside incident response vendors, law enforcement, and other stakeholders. In coordination with your attorney, get to know your Sheriff/City police, and your [State’s Fusion Center](https://www.dhs.gov/fusion-center-locations-and-contact-information). Emergency managers may have a continuity plan that your CIRP can tie into.

***Meet your CISA regional team***.

You can find your CISA [regional office information](https://www.cisa.gov/cisa-regions) here. Within each CISA Region are your local and regional Protective Security Advisors (PSAs), Cybersecurity Advisors (CSAs), Election Security Advisor (ESA), Emergency Communications Coordinators, and other CISA personnel to handle a wide array of needs.

## During a cybersecurity incident

***Remain calm.***

Follow the plan, use it as a guide.

***Should Incident Manager, Tech Manager not be available:***

Leave them a short message and continue to contact key staff, in particular backup managers, IT contacts or emergency manager.

***Considerations for the Incident Manager (IM):***

* Setup initial meeting with key contacts and Tech Manager.
* Assess key critical services and their availability to establish full impact of incident and communicate it to Tech Manager.
* Consider time frame for ongoing updates to key required contacts, and all other necessary key contacts., until incident is declared over.
* Consider leveraging Microsoft Teams or other collaborative application that is available to internal staff. The IM or Communications Manager can build this group in Teams ahead of time or quickly during the incident. These tools can be a great source to document all activities that are taking place and can be used later for documenting the steps taken during the incident.
* When there is time, IM or CM should complete the Incident Response Report to document what is known and update with timestamps as time allows. The Tech Manager can review and edit when they have time (which may be after the incident is declared over by the IM).

# After a cybersecurity incident

***Hold a hotwash meeting (sometimes called a “retrospective” or “after actions”)***.

In the retrospective, the IM will report out the known incident timeline and ask for additions and edits. They will then ask for analysis from the incident response team and suggest areas for improvement.

**Note:** The hotwash must be blameless. For a hotwash to have any value, all participants need to feel free to openly discuss the incident in a safe and supportive environment. Security incidents are rarely the result of one person’s action. They are almost always the result of a failure of the overall system. The hotwash will examine people, processes, and technologies. The focus should be on the processes and ways to improve them.

***Review any documents used during the incident.***

Review Key Contacts, Key Critical Services, and Incident Response Reports. Do not alter the originals but create a final draft with updated and accurate information. Share with Key Contacts or relevant staff and hotwash team members. Archive all documentation used during the incident according to records retention laws or policies.

***Update policies, procedures, IR templates.***

As needed and based on the hotwash meeting, update policies, procedures, templates, and other details in the CIRP.

***Communicate the findings to your staff.***

Transparency builds trust and many staff will appreciate hearing how seriously the executives consider security, which is a major step in building a culture of security.



# Cyber Incident Response Templates

Some of these templates may not be practical to implement for your organization. Use accordingly to create, modify, and/or add to your existing CIRP.

# Executive Support, Responsibility, History, Change Log

**Executive Support***List the executives who provided input to this document and endorsed its development and applicability.*

|  |  |  |
| --- | --- | --- |
| Date | Name of Executive | Signature |
|  |  |  |

**Assignment of Responsibility***List employees at your organization who are responsible for developing and maintaining this plan.*

|  |  |  |
| --- | --- | --- |
| Date | Name of Employee | Responsibility |
|  |  |  |

**History of Test or Exercise of This Plan**

|  |  |  |
| --- | --- | --- |
| Date | Event | Comment |
| 08/01/24 | Example: CISA Cyber TTX | Example: See after actions report and notes for future updates |

**Incident Response Plan Change Log**

|  |  |  |
| --- | --- | --- |
| Date | Event | Comment |
| 08/01/24 | Incident Response Plan Created |  |

Incident Prioritization Impact levels  
(Based on [NIST SP800-61R2 Computer Security Incident Handling Guide](https://csrc.nist.gov/pubs/sp/800/61/r2/final) - page 41 Section 3.2.6 Incident Prioritization.)

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis due to resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following Functional, Information and Recoverability categories to help determine the business impact of the incident. It’s recommended that each organization define and exercise on these impact levels.

|  |  |
| --- | --- |
| **Functional Impact** | Definition |
| None | No effect to the organization’s ability to provide services to all users |
| Low | Minimal effect to the organization. Can still provide all critical services to all users but has lost efficiency. |
| Medium | Organization has lost the ability to provide a critical service to a subset of system users. |
| High | Organization is no longer able to provide some critical services to any users. |
| **Information Impact** | Definition |
| None | No information was exfiltrated/leaked, disclosed, changed, deleted, used, or disclosed by or for unauthorized persons or purposes, or otherwise compromised. |
| Privacy Breach | Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc., was accessed or exfiltrated/leaked, or protected health information (PHI) of individuals was used or disclosed by or for unauthorized persons or purposes, or otherwise compromised. |
| Proprietary Breach | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed, exfiltrated/leaked, or used or disclosed by or for unauthorized persons or purposes. |
| Integrity Loss (based on Functional Impact) | Sensitive or proprietary information was changed or deleted accidentally or intentionally. |
| **Recoverability Effort** | Definition |
| Regular | Time to recovery is predictable with existing resources. |
| Supplemented | Time to recovery is predictable with additional resources. |
| Extended | Time to recovery is unpredictable; additional resources and outside help are needed. |
| Not recoverable | Recovery from the incident is not possible (e.g., sensitive data exfiltrated/leaked and posted publicly); launch investigation. |

# ****Key Contacts****

| **Job Title/Role** | **Name** | **Phone Number(s)  (Office, Cell, Home)** | **Email (organizational & personal)** | **Notify:** | **Additional Note(s):** |
| --- | --- | --- | --- | --- | --- |
| **Incident Manager (IM)** |  |  |  |  | **Essential Role. Need an alternate if not available.** |
| **Tech Manager (TM)** |  |  |  |  | **Essential Role. Need an alternate if not available.** |
| **Communications Manager (CM)** |  |  |  |  | **Essential Role. Need an alternate if not available.** |
| **Office Manager** |  |  |  |  |  |
| **IT Contact** |  |  |  |  |  |
| **Emergency Manager** |  |  |  |  |  |
| **Office Staff** |  |  |  |  |  |
| **Legal Counsel** |  |  |  |  |  |
| **Stakeholder who requires notification of plan activation** |  |  |  |  |  |
| **External Support for information asset** |  |  |  |  |  |
| **External Support for technology asset** |  |  |  |  |  |
| **Local Law Enforcement** |  |  |  |  |  |
| **Fire Department** |  |  |  |  |  |
| **Phone Company** |  |  |  |  |  |
| **Power Company** |  |  |  |  |  |
| **Internet Service Provider** |  |  |  |  |  |
| **Cyber Insurance** |  |  |  |  |  |
| **Website Host / Developer** |  |  |  |  |  |
| State Fusion Center | Montana Analysis and Technical Information Center | 406-444-1330 | dojintel@mt.gov |  | [Fusion Center Locations](https://www.dhs.gov/fusion-center-locations-and-contact-information) |
| **Cybersecurity & Infrastructure Security Agency (**CISA**)** |  | **1-844-Say-CISA 1-844-729-2472** | [SayCISA@cisa.gov](mailto:SayCISA@cisa.gov) |  | [Report Incident](https://myservices.cisa.gov/irf) per online form or Email [SayCISA@cisa.dhs.gov](mailto:SayCISA@cisa.dhs.gov)  For more info – [CISA.GOV](https://www.cisa.gov/) |
| **CISA -Cyber State Coordinator (CSC)** | **Joe Frohlich** | **406-461-2651** | **Joseph.frohlich@mail.cisa.dhs.gov** |  |  |
| **CISA -Cybersecurity Advisors (CSA)** | **Travis Light** | **406-894-8374** | **Travis.light@mail.cisa.dhs.gov** |  |  |
| **CISA – Protective Security Advisor (PSA)** | **Randy Middlebrook** | **406-839-1165** | **Randy.Middlebrook@mail.cisa.dhs.gov** |  |  |
| **CISA – Protective Security Advisor (PSA)** | **Albert Mendoza** | **406-371-3585** | **Albert.Mendoza@mail.cisa.dhs.gov** |  |  |
| **MS-ISAC (Multi State Information Sharing and Analysis Center** |  | **1-866-787-4722** | [soc@cisecurity.org](mailto:soc@cisecurity.org) |  | [MS-ISAC](https://www.cisecurity.org/ms-isac)  Not your sectors ISAC? Find yours at [National Council of ISACs](https://www.nationalisacs.org/) |
| **FBI Field Office** | **Salt Lake (MT, ID, UT)** | **801-579-1400** |  |  | [Field Offices — FBI](https://www.fbi.gov/contact-us/field-offices) |
| **Regulatory org that requires notification** |  |  |  |  |  |

# Communication Channels to Notify Key Contacts and Stakeholders

*To report a possible incident and possibly stand up the IR Team*

| **Call** | **Email** | **Text** | **Report to a location** | **Details** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

*If applicable: When Incident Commander approves to notify Cyber Insurance or 3rd party IR Team*

| **Cyber Insurance / 3rd Party IR Team** | **Phone Number** | **Contact** | **Who makes the call** | **Details** |
| --- | --- | --- | --- | --- |
|  |  |  | **Example: Incident Commander** | **Example: M-F 0800-1700 call main line** |

*Communication channels to be used to notify stakeholders if this plan is to be executed.*

| **Order of communication attempts to key contacts** | **Communication methods to Key Contacts** | **Alert Message Header** | **Test Alert Message Header** | **Details** |
| --- | --- | --- | --- | --- |
| **1** | **Incident alert system** |  |  | **Example: This system will call/text** |
| **2** | **Cellphone** |  |  |  |
| **3** | **Email** |  |  |  |
| **4** | **SMS/Text** |  |  |  |
| **6** | **Collaboration tool** |  |  | **(Example: Use the existing Microsoft Teams IR channel for remote meetings, file share and discussion)** |
| **7** | **Collaboration tool** |  |  | **(Example: Google Workspace IR channel)** |
| **8** | **Telephone** |  |  |  |
| **9** | **Physical Primary meeting location** |  |  | **significate event and all communications are down – meet physically here in room XXXX. IC or designee team member will post next meeting time(s).** |
| **10** | **Physical Secondary meeting location** |  |  |  |

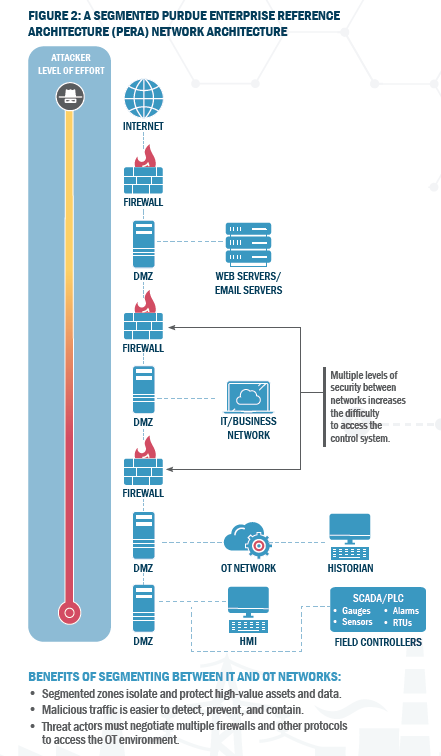
# ****Essential Assets****

| **Essential IT Asset** | **Availability** | **IP Address** | **Backup information (location, schedule, date last run)** | **Additional Details as needed: Examples:** Vendor, Model**,** Firmware**,** OS **Version,** system administrator (SA) **account(s),** AV, AV **Version & AV signature file date, Last** Patch Date, Last **Firmware update date, Last** Configuration **Date, Last** Maintenance date, On Premise or Cloud |
| --- | --- | --- | --- | --- |
| **Firewall** | **Up | Partial | Down** |  |  |  |
| **Router** | **Up | Partial | Down** |  |  |  |
| **Switch** | **Up | Partial | Down** |  |  |  |
| **Intrusion/Prevention Detection System** | **Up | Partial | Down** |  |  |  |
| **Virtual Machine Environment** | **☐Up | ☐Partial | ☐Down** |  |  |  |
| **Domain Controller** | **Up | Partial | Down** |  |  |  |
| **AD Domain Controller** | **Up | Partial | Down** |  |  |  |
| **DNS / DHCP server** | **Up | Partial | Down** |  |  |  |
| **SIEM Server** | **Up | Partial | Down** |  |  |  |
| **Event Log Server** | **Up | Partial | Down** |  |  |  |
| **MFA Server/Appliance** | **Up | Partial | Down** |  |  |  |
| **File Server** | **Up | Partial | Down** |  |  |  |
| **Data Storage** | **Up | Partial | Down** |  |  |  |
| **Network Attached Storage** | **Up | Partial | Down** |  |  |  |
| **Database Server** | **Up | Partial | Down** |  |  |  |
| **Email Server** | **Up | Partial | Down** |  |  |  |
| **Email Security Gateway** | **Up | Partial | Down** |  |  |  |
| **Web Server** | **Up | Partial | Down** |  |  |  |
| **Web Application Firewall** | **Up | Partial | Down** |  |  |  |
| **Web Filter Appliance** | **Up | Partial | Down** |  |  |  |
| **Print Server** | **Up | Partial | Down** |  |  |  |
| **Backup Appliance** | **Up | Partial | Down** |  |  |  |
| **VPN Appliance** | **Up | Partial | Down** |  |  |  |
| **VOIP / Telephone** | **Up | Partial | Down** |  |  |  |
| **Wireless Controller** | **Up | Partial | Down** |  |  |  |
| **Wireless Access Point** | **Up | Partial | Down** |  |  |  |
| **Essential Workstation** | **Up | Partial | Down** |  |  |  |
| **Vulnerability Scanning Server** | **Up | Partial | Down** |  |  |  |
| **Patch Management Server** | **Up | Partial | Down** |  |  |  |
| **Phone System** | **Up | Partial | Down** |  |  |  |
| **Website** | **Up | Partial | Down** |  |  |  |
| **Critical Service** | **Up | Partial | Down** |  |  |  |
| **Cloud Service** | **Up | Partial | Down** |  |  |  |
| **Other locations or Offices** | **Up | Partial | Down** |  |  |  |
| **Printers** | **Up | Partial | Down** |  |  |  |
| **Copiers** | **Up | Partial | Down** |  |  |  |

# ****Essential Operational Technology (OT) Assets****

| **Essential OT Asset** | **Availability** | **IP Address** | **Backup information (location, date last run)** | **Additional Details as needed: Examples: Vendor, Model, Firmware, OS Version, system administrator (SA) account(s), AV, AV Version & AV signature file date, Last Patch Date, Last Firmware update date, Last Configuration Date, Last Maintenance date** |
| --- | --- | --- | --- | --- |
| **Historian** | **Up | Partial | Down** |  |  |  |
| **Data Acquisition** | **Up | Partial | Down** |  |  |  |
| **Human Machine Interface (HMI)** | **Up | Partial | Down** |  |  |  |
| **Distributed Control System (DCS)** | **Up | Partial | Down** |  |  |  |
| **Supervisory Control and Data Acquisition (SCADA)** | **Up | Partial | Down** |  |  |  |
| **Remote Telemetry Unit (RTU)** | **Up | Partial | Down** |  |  |  |
| **Modem Pool / PBX** | **Up | Partial | Down** |  |  |  |
| **Sensors** | **Up | Partial | Down** |  |  |  |
| **Intelligent Electronic Device (IED)** | **Up | Partial | Down** |  |  |  |
| **Programmable Logic Controller (PLC)** | **Up | Partial | Down** |  |  |  |
| **Engineering Workstation** | **Up | Partial | Down** |  |  |  |
| **Control Room Workstation** | **Up | Partial | Down** |  |  |  |
| **Backup Appliance** | **Up | Partial | Down** |  |  |  |
| **Database Server** | **Up | Partial | Down** |  |  |  |
| **Backup Appliance** | **Up | Partial | Down** |  |  |  |
| **VPN Appliance** | **Up | Partial | Down** |  |  |  |
| **VOIP / Telephone** | **Up | Partial | Down** |  |  |  |
| **Wireless Controller** | **Up | Partial | Down** |  |  |  |

# ****Simple Network Diagram****

****

**[Remove above network diagram and insert your organization’s IT or OT network diagram or attach to Appendix at end of CIRP. Diagram on left was created by using CISA’s free** [Cyber Security Evaluation Tool](https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset) **(CSET). Once CSET is downloaded search Network Diagram in “Assessments.” Figure 2 on the right is network security recommendations from CISA’s infographic:** [Layering Network Security Through Segmentation](https://www.cisa.gov/resources-tools/resources/layering-network-security-through-segmentation-infographic)**]**

# ****Essential Software, Applications and Licensing****

| **Essential Software, App / Licensing** | **Applies to:** | **Website / download portal** | **Downloaded/Backup Location** | **Licensing Information Details: (Keys, Contact, Phone Support #s, etc.)** |
| --- | --- | --- | --- | --- |
| **Anti-Virus -Endpoint Detection Remediation** | **All Systems |  Other:** |  |  | **(Example: Licensing printout information can be found in Appendix at the end of this CIRP)** |
| **Microsoft Windows** | **All Systems |  Other:** |  |  |  |
| **Linux** | **All Systems |  Other:** |  |  |  |
| **End User Training** | **All Systems |  Other:** |  |  |  |
| **Microsoft O365** | **☐ All Systems | ☐ Other:** |  |  |  |
| **Software Vendor** | **All Systems |  Other:** |  |  |  |
| **Application Vendor** | **All Systems |  Other:** |  |  |  |
| **Cloud App Vendor** | **All Systems |  Other:** |  |  |  |

# ****Primary and Alternate Sites****

| **Site Name:** | **Physical Location** | **Location Type** | **Site Type ( NIST Definitions** [Hot Site](https://csrc.nist.gov/glossary/term/hot_site)**,** [Warm Site](https://csrc.nist.gov/glossary/term/warm_site)**,** [Cold Site](https://csrc.nist.gov/glossary/term/cold_site)**. )** | **Date Failover Exercised/Tested** |
| --- | --- | --- | --- | --- |
|  |  | **Primary |  Alternate** | **Hot |  Warm | Cold | Details:** |  |
|  |  | **Primary |  Alternate** | **Hot |  Warm | Cold | Details:** |  |
|  |  | **Primary |  Alternate** | **Hot |  Warm | Cold | Details:** |  |
|  |  | **Primary |  Alternate** | **Hot |  Warm | Cold | Details:** |  |
|  |  | **Primary |  Alternate** | **Hot |  Warm | Cold | Details:** |  |
|  |  | **Primary |  Alternate** | **Hot |  Warm | Cold | Details:** |  |

Asset Backup Information Details

| **Asset Type** | **Backup Solution** | **Backup Frequency:** | **Backup Retention** | **Physical / Logical Location(s)** | **Last Tested Date** | **Backup Details (**Encryption**,** Immutable**, Offline, Tested no less than 1 year)** | **Additional Backup Notes** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Server(s)** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** |  |
| **Workstation(s)** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** |  |
| **Switch(s)** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** |  |
| **Firewalls(s)** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** |  |
| **Network Diagram** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** |  |
| **OT Diagram** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** |  |
| **Operational Technology (OT) Assets** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** | **[Examples include configurations, roles, programmable controller (PLC), engineering drawings, and tools]** |
| **Gold Images or** [**Baseline Configurations**](https://csrc.nist.gov/glossary/term/baseline_configuration) **for critical systems** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** | **[Examples include image “templates” that have a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system.]** |

|  |  |
| --- | --- |
| Incident Reporting Template Based on [CISA Cyber Resilience Review Supplemental Resource Guides](https://www.cisa.gov/resources-tools/resources/cyber-resilience-review-supplemental-resource-guides), Incident Management page 42 | |
| **Reporting Staff & Date** | |
| Today’s Date: |  |
| Name of individual completing this form: |  |
| Job Title/Role: |  |
| Contact Information (email/phone): |  |
| **Incident Short Summary** (1 or 2 sentences) | |
|  | |
| **Incident Priority** | |
| None  Low  Medium  High | |
| **Incident Type** | |
| Compromised System |  Compromised User Credentials (e.g., lost password) |  Network Attack (e.g., DoS) | Malware (e.g., virus, worm, Trojan) |  Reconnaissance (e.g., scanning, sniffing) |  Lost Equipment/Theft |  Physical Break-in |  Social Engineering (e.g., Phishing)  Law Enforcement Request |  Policy Violation (e.g., acceptable use) |  Unknown/Other (Please describe below.) | |
| **Incident Timeline** | |
| Date and time when the incident was discovered: |  |
| Date and time when the incident was reported: |  |
| Date and time when the incident occurred: |  |
| **Incident Scope** | |
| Estimated number of systems affected: |  |
| Estimated number of users affected: |  |
| Third parties involved or affected (e.g., vendors, contractors, partners): |  |
| **Systems Affected by the Incident** | |
| Primary functions of the affected systems (e.g., web server, domain controller): |  |
| Any sensitive information known to be stored on affected systems? (PII, PHI, CJIS, FTI, etc.) |  |
| Attack sources (e.g., IP address, port): |  |
| Attack destinations (e.g., IP address, port): |  |
| IP addresses of the affected systems: |  |
| Operating systems of the affected systems (e.g., version, service pack, patch level, configuration): |  |
| Security software loaded on the affected systems (e.g., anti-virus, anti-spyware, firewall, versions, date of latest definitions): |  |
| Physical location of the affected systems (e.g., state, city, building, room, desk): |  |
| **Users Affected by the Incident** | |
| Names and job titles of the affected users: |  |
| System access levels or rights of the affected user (e.g., regular user, domain administrator, root): |  |
| **Incident Handling Log** | |
| Actions taken to identify the affected resources: |  |
| Actions taken to remediate the incident: |  |
| Actions planned to prevent similar incidents |  |
| **Review key contacts information and identify who the Communications Manager is to notify by checking the appropriate box.** | |
| **Additional Notifications** | |
| None |  IT |  Leadership |  Emergency Manager |  Legal Counsel  Law Enforcement |  Fusion Center |  STATE |  CISA |  MS-ISAC | |
| **Is there a need for help or assistance? (From: State, Fusion Center, CISA)** | |
| Yes | No | Note: | |

# **Internal policies, laws, rules, regulations, and breach notification requirements**

|  |  |  |  |
| --- | --- | --- | --- |
| **Internal Policies** | **Links** | **Requirement** | **Notes** |
|  |  |  |  |
|  |  |  |  |
| **Laws, rules and/or regulations** | **Links** | **Requirement** | **Notes** |
| Example: Health Insurance Portability and Accountability Act (HIPAA) | [Summary of the HIPAA Privacy Rule | HHS.gov](https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)  [Breach Reporting | HHS.gov](https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html) | Notify individual or Covered Entity of a breach of unsecured protected health information (PHI) which poses a significant risk of financial, reputational, or other harm to the individual. Individual notice must contain certain mandatory media notices (involving 500 or more individuals) as soon as possible but no later than 60 days from discovery of the breach. | Applies only to HIPAA Covered Entities and HIPAA-protected health information. A Business Associate of a Covered Entity is required to notify the Covered Entity as soon as possible but no later than 60 days from the discovery of the breach. Contracting for a shorter time is a best practice. |
| Example: Montana Code Annotated 2023 – Computer Security Breach | [30-14-1704. Computer security breach, MCA](https://archive.legmt.gov/bills/mca/title_0300/chapter_0140/part_0170/section_0040/0300-0140-0170-0040.html) |  | Example of Montana State Law |

# ****Additional Incident Report Considerations and Questions****

[Modify as needed. Could be used for a quick initial IR Reporting for multiple uses, such as help desk, end users, etc.]

| **Question** | **Additional Details:** | **Availability** |
| --- | --- | --- |
| **Is there power?** | Yes | No | Note: | **Fully Available | Partially Available | Unavailable** |
| **Is there internet access?** | Yes | No | Note: | **Fully Available | Partially Available | Unavailable** |
| **Is there access to essential work applications?** | Yes | No | Note: | **Fully Available | Partially Available | Unavailable** |
| **Is there access to work files?** | Yes | No | Note: | **Fully Available | Partially Available | Unavailable** |
| **Is there telephone access?** | Yes | No | Note: | **Fully Available | Partially Available | Unavailable** |
| **Is there cell service?** | Yes | No | Note: | **Fully Available | Partially Available | Unavailable** |

# Communication Templates

These templates are available to help Communications Manager (CM) manage communications during incidents that impact operations or security. Each template includes instructions and considerations for effective communication, maintaining transparency, and ensuring accurate and timely updates. Customize the templates with specific details relevant to the incident and your organization. These templates are designed to align with the best practices outlined in this guide.

Below are communication functions to consider for your Incident Response Team. Understanding that teams are often small, many of these functions may be filled by the same person.

* **Communications Manager** **/Lead Spokesperson** – During an incident consider a senior leader in the organization for this function, who can speak on the record, with authority and has a good understanding of not only the incident, but the framework and processes potentially impacted.
* **Onsite-Incident Lead** – This individual would be onsite to interface with the individuals managing the response.
* **Communications Planner(s)** – e.g., Incident, strategic, internal.
* **Digital** (Website / Social Media) **Manager**

**The following templates are included:**

**Initial Incident Notification Template** (Non Public)

**Purpose:** Quickly inform key stakeholders about an incident and initial details.

**Use:** Internal and external partners and stakeholders only; not for public dissemination.

**Public Statement Template**

**Purpose:** Acknowledge an incident and provide initial public-facing information.

**Use:** Broader audience including the public and media.

**Public Update Checklist**

**Purpose:** Checklist to determine when to update the public.

**Use:** Ensure timely and necessary updates to the public.

**Public Information (Press) Release Template** – **Talking Points Guide**

**Purpose:** Ensure consistent and accurate public communication.

**Use:** Media interactions and public updates.

# Initial Incident Notification Template (Non-Public)

**Purpose**

This template is designed to quickly inform internal and external partners and stakeholders about an incident impacting operations or security. It ensures timely, accurate, and concise communication during the critical early stages of an incident response, specifically for those directly involved in managing the incident; not for public dissemination.

**Instructions/Considerations**

Before sending the notification, ensure you have verified the key facts about the incident. Keep the message brief but informative, focusing on essential details. Tailor the message for different stakeholders as needed, ensuring all relevant parties receive appropriate information and emphasize that information should not be disclosed publicly.

**Email**

**Subject:** Immediate Notification of Incident

**Date and Time:** [Insert Date and Time]

**From:** [Communications Manager/Official’s Name]

**To:** [List of Recipients - Internal Stakeholders, Law Enforcement, CISA, etc.]

Good [Morning/Afternoon/Evening],

Our office has [observed/received a report of] an incident that could impact operations. While our office is in the process of gathering additional details, we are writing to provide a brief update about what we know currently. This information is for your awareness only and not for further dissemination or public release.

**Incident Summary Type of Incident:** [Severe weather, cyber incident, equipment malfunction, etc.]

**Date and Time of Incident:** [Insert date and time]

**Location:** [Insert location]

**Current Status:** [Brief description of incident status]

**Known Facts:** [Only include information that is available and appropriate to share at this time.]

**What Happened:** [Brief description of the incident]

**Impact on Operations:** [Details about how the incident has affected or may affect operations]

**Immediate Actions being Taken:** [Description of any immediate steps taken to address the incident (i.e., who has been notified; assessment of critical comms systems; coordination with law enforcement and state and federal partners, as necessary.]

As per our incident response plan, we have activated the necessary protocols to respond to the incident. We will continue to investigate the incident and provide updates as more information becomes available. Our priority is to ensure the integrity and continuity of operations while keeping all stakeholders informed.

**Points of Contact** For further information or to report additional details, please contact:

**Primary Contact:** [Name, Title, Phone, Email]

**Secondary Contact:** [Name, Title, Phone, Email]

Thank you,

[Email Signature]

# Holding Statement Templates

**Purpose**

A public statement, or holding statement, serves as an initial incident notification to a broader audience, including the public. A holding statement is used after an incident has been initially reported, but before complete information is available. Holding statements provide a way to keep stakeholders and the public informed while incident response is underway. The statement acknowledges the incident, assures the public and stakeholders that it is being addressed, and reiterates commitment to providing further updates as the situation develops.

**Instructions/Considerations**

Before sending a holding statement, ensure you have verified the key facts about the incident. Keep the message brief and avoid including every detail. The purpose is to alert stakeholders and the public that you are aware of the incident and are actively responding to it. Be mindful: these communications are public facing. Ensure the information shared is accurate and contains an appropriate level of detail for public consumption. Plan to provide follow-up updates as more information becomes available.

**Social Media Posts**

**Facebook/X/Instagram:**

We are aware of an incident affecting [insert brief description here]. Our team is actively responding and coordinating with [insert Cyber Insurance or the appropriate authorities]. We will provide updates as more information becomes available. For further details, visit [Organization Website].

**Website Alert/Banner**

We are aware of an incident affecting [insert brief description here]. Our team is actively responding and coordinating with [insert Cyber Insurance or the appropriate authorities]. We will provide updates as more information becomes available. We will provide updates as more information becomes available. Contact: [Primary Contact Information]

**Contact Information:**

* **Primary Contact:** [Name, Title, Phone, Email]
* **Secondary Contact:** [Name, Title, Phone, Email]

Thank you,

**Email**

**Subject:** Incident Acknowledgement and Initial Response

**Date and Time:** [Insert Date and Time]

**From:** [Organization/Official Name]

**To:** [List of Recipients - Internal Stakeholders, Law Enforcement, CISA, Public, etc.]

Good [Morning/Afternoon/Evening],

[Organization] is aware of an incident which as occurred affecting our [insert brief description here]. At this moment, our team continues to actively investigate the situation and take necessary response actions. Here is what we know so far:

**Incident Summary:**

**Incident Type:** [Severe weather, cyber incident, equipment malfunction, etc.]

**Date and Time of Incident**: [Insert Date and Time]

**Location:** [Insert Location]

**Current Status**: [Only include information that is available and appropriate to share at this time.]

**Description of Incident:** [Brief description]

**Immediate Actions Taken:** [Any immediate steps taken (i.e., activated incident response plan; coordinating with Cyber Insurance, local law enforcement, Federal Partners)]

**Next Steps:**

We will provide additional information as it becomes available. Further updates will be communicated through [specific channels, e.g., email, website, social media, press releases]. We want to assure the public that we are taking this incident seriously and are committed to quickly resolving the incident while maintaining the safety and privacy of our partners.

**Points of Contact:** For any inquiries, please contact:

**Primary Contact:** [Name, Title, Phone, Email]

**Secondary Contact:** [Name, Title, Phone, Email]

Thank you,

[Email Signature]

# Public Information Release Template – Talking Points Guide

**Purpose**

This template provides key talking points to use when communicating with the media and public during an incident. These points ensure consistent and accurate messaging and are aimed at maintaining public confidence and transparency.

**Instructions/Considerations**

Before using these talking points, ensure they are updated with the most current and accurate information about the incident. Be mindful of the public facing nature of these communications, and tailor the level of detail accordingly.

**Talking Points**

**Incident Overview:**

* We are aware of an incident affecting [insert brief description here] and are actively responding.
* Our priority is to ensure the security and integrity of….

**Current Status:**

* Incident Type: [Brief description of the type of incident]
* Date and Time: [Insert Date and Time of the incident]
* Location: [Insert Location]

**Impact on Operations:**

* We are assessing the impact on [insert brief description here such as] and will provide updates as more information becomes available.
* [Specific impact details, e.g., changes, delays]
* As applicable, outline security measures in place to ensure the integrity of the process to put the incident in context for the public.

**Response Efforts:**

* We have activated our incident response plans.
* [High level response activities that are underway, e.g., we are coordinating with law enforcement; we are in communication with staff on location and receiving regular updates]
* As applicable, outline how your actions are continuing to ensure the security and integrity of the process.

**Public Assurance:**

* The [insert a few high-level current priorities that you are wanting the public to know], are our top priorities.
* We are committed to transparency and will provide timely updates as the situation develops.

**Responding to Speculation and Next Steps:**

* Our office is actively coordinating with [insert appropriate authorities] to [insert appropriate action like investigate, restore service, etc.].
* We appreciate your patience as we address the situation and ensure that necessary actions are taken to ensure the restoration of our operations.
* We will continue to assess the situation and respond accordingly.
* Further updates will be communicated through our website and social media channels.

**Contact Information:**

For further inquiries, please contact [Primary Contact Name, Title, Phone, Email].

# Key Terms

Add to or Edit to define for your organization.

| **Term** | **Definition:** | **Source** |
| --- | --- | --- |
| Breach | The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose. | <https://csrc.nist.gov/glossary/term/breach> |
| Event | Any observable occurrence in a network or system. | <https://csrc.nist.gov/glossary/term/event> |
| Impact | The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. | <https://csrc.nist.gov/glossary/term/impact> |
| Incident | An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. | <https://csrc.nist.gov/glossary/term/incident> |
| Risk | A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. | <https://csrc.nist.gov/glossary/term/risk> |
| Vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. | <https://csrc.nist.gov/glossary/term/vulnerability> |

# References

* [CISA Incident Response Plan Basics](https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf)
  + Used in this guide for:
    - Communication Channels to be used during an incident
    - Best Practices
* [Federal Government Cybersecurity Incident and Vulnerability Response Playbooks](https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks)
  + Used in this guide for:
    - Executive Support, Responsibility, History, Change Log
    - Key Contacts
    - Communication Channels to be used during an incident
    - Key Essential Assets
    - Key Essential Operational Technology (OT) Assets
    - Incident Response Preparation Checklist
    - Incident Response Checklist
    - Vulnerability Response Playbook
* [NIST SP 800-61 Rev.2 – Computer Security Incident Handling Guide](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)
  + Used in this guide for:
    - Incident Reporting Template
    - Incident Prioritization Key Terms
      * Page 41 within SP 800-61 Section 3.2.6
* [NIST Glossary terms and definitions](https://csrc.nist.gov/glossary)
  + Used in this guide for:
    - Key Terms
* [#StopRansomware Guide](https://www.cisa.gov/resources-tools/resources/stopransomware-guide)
  + Used in this guide for: Asset Backup Information Details
* [CISA Cyber Resilience Review Supplemental Resource Guides](https://www.cisa.gov/resources-tools/resources/cyber-resilience-review-supplemental-resource-guides) – Incident Management
  + Used in this guide for:
    - Executive Support, Responsibility, History, Change Log
    - Key Contacts
    - Communication Channels to be used during an incident
    - Key Essential Assets
    - Key Essential Operational Technology (OT) Assets
    - Incident Reporting Template
* [Layering Network Security Through Segmentation](https://www.cisa.gov/resources-tools/resources/layering-network-security-through-segmentation-infographic)
  + Used in this guide for: simple Network/OT Diagram
* CISA [Cyber Security Evaluation Tool](https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset) (CSET)
  + Used in this guide for: simple Network/OT Diagram
* [CISA Election Infrastructure Incident Response Communications Guide](https://www.cisa.gov/resources-tools/resources/election-infrastructure-incident-response-communications-guide)
  + Used in the guide for:
    - Initial Incident Notification Template (Non-Public)
    - Public Holding Statement Templates
    - Public Information Release Template – Talking Points Guide