[Insert Organization] Incident Response Plan



[Remove and insert your organizations logo]

[CISA Cybersecurity Incident Response Plan Basic Templates (Version 2025-04)]

Version: 2025-07-14

Confidential

# Introduction

A Incident Response Plan (IRP) 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 IRP 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 basic IRP presents templates to quickly get started on your organization’s IRP, or to enhance your existing IRP. It is recommended that you review this document completely. Some of these templates may not be practical to implement for your organization. Use accordingly to create, modify, and/or add to your existing IRP.

If you do not have an IRP:

* 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 IRP 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 IRP Team who have a need to know.
* Train staff on the IRP 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 IRP:

* Compare your IRP with the provided templates
* Identify and document possible areas for improvement.

As you are creating or updating your IRP, 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 organizations or departments with little or no dedicated IT and/or Security staff or for those that use an IT Managed Service Provider. A similar small, mid to large organization IT templates has been created for more detailed guidance and preparation activities. Contact your local CISA Cybersecurity Advisor for questions or additional resources.

# 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 |  |

# ****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** |  |  |  |  |  |

# ****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 |
| --- | --- | --- | --- | --- |
| **Critical Service/App** | **Up | Partial | Down** |  |  |  |
| **Cloud Service** | **Up | Partial | Down** |  |  |  |
| **File Storage** | **Up | Partial | Down** |  |  |  |
| **Email** | **Up | Partial | Down** |  |  |  |
| **Essential Workstation** | **Up | Partial | Down** |  |  |  |
| **Phone System** | **Up | Partial | Down** |  |  |  |
| **Website** | **Up | Partial | Down** |  |  |  |
| **Other locations or Offices** | **Up | Partial | Down** |  |  |  |
| **Printers** | **Up | Partial | Down** |  |  |  |
| **Copiers** | **Up | Partial | Down** |  |  |  |

# ****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:** |  |

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** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **File Store** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** |  |
| **Critical Application** |  |  |  |  |  | **encrypted |  Immutable |  maintain offline copy|  regularly tested** |  |

|  |  |
| --- | --- |
| 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.) |  |
| 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: |  |

# ****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** |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Internal Policies** | **Links** | **Requirement** | **Notes** |
|  |  |  |  |
|  |  |  |  |
| **Laws, rules and/or regulations** | **Links** | **Requirement** | **Notes** |
| 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 |