



CITY CYBERSECURITY INCIDENT

RESPONSE PLAN TEMPLATE

|  |
| --- |
| **<Indiana City>** |
| *Cybersecurity Incident Response Plan* |
| Annex to the City EOP |
| <<Lead Department>> |
| WORKING DRAFT |

|  |
| --- |
|  |

[I. INTRODUCTION 4](#_Toc149051220)

[A. PURPOSE 4](#_Toc149051221)

[B. SCOPE 4](#_Toc149051222)

[C. SITUATION OVERVIEW 5](#_Toc149051223)

[II. INCIDENT RESPONSE 6](#_Toc149051224)

[A. Team Organization 6](#_Toc149051225)

[1. Cyber Incident Response Team 6](#_Toc149051226)

[2. Policy Group 9](#_Toc149051227)

[3. Communications 9](#_Toc149051228)

[4. Information Technology and Cyber Response 10](#_Toc149051229)

[B. Cyber Incident Severity Levels 10](#_Toc149051230)

[C. Cyber Incident Lifecycle Overview 12](#_Toc149051231)

[D. Detection of a Cyber Incident 12](#_Toc149051232)

[1. Recognition of a potential incident 12](#_Toc149051233)

[E. Cyber Incident Response Tasks RESPONSE – START HERE! 13](#_Toc149051234)

[1. Upon Detection and Notification to the Cyber Incident Response Team 13](#_Toc149051235)

[2. Mitigation and Recovery 14](#_Toc149051236)

[3. Continued Operational Periods Planning (IAP) 16](#_Toc149051237)

[4. Update Response and Recovery Recommendations 16](#_Toc149051238)

[F. Demobilization 17](#_Toc149051239)

[III. Cyber Incident Response Team Assignment Form 19](#_Toc149051240)

[IV. Cyber Incident Reporting Guidance 20](#_Toc149051241)

[A. Definitions – Cyber Emergency vs. Cyber Incident, IOT 20](#_Toc149051242)

[B. State Level Event Reporting 20](#_Toc149051243)

[C. Law Enforcement Event Reporting 20](#_Toc149051244)

[D. Additional Resources During a Cyber Event 21](#_Toc149051245)

[E. Information Sharing 22](#_Toc149051246)

[V. Indiana Regulatory Codes and Industry Standards 22](#_Toc149051247)

[A. Indiana Codes 22](#_Toc149051248)

[B. Industry Standards 29](#_Toc149051249)

[VI. Cyber Incident Continuity of Operations Assessment 30](#_Toc149051250)

[VII. Cyber Incident Response Team Members 31](#_Toc149051251)

[VIII. Internal Notification Parties 33](#_Toc149051252)

[IX. External Notification Parties 34](#_Toc149051253)

[X. Operational Planning Process 35](#_Toc149051254)

[XI. Incident Action Plan Forms 44](#_Toc149051255)

[A. Incident Action Plan (IAP) Quick Start 44](#_Toc149051256)

[B. Activity Log 46](#_Toc149051257)

[C. ICS 213 General Message Form 48](#_Toc149051258)

# INTRODUCTION

## PURPOSE

In recognition of the growing everyday threat of a cyber security incident, this Cyber Incident Response Plan was developed to provide the foundational guidance for the planning, preparing, responding, and recovery actions.

The plan is organized by first providing an overview of the plan’s concept of operations, followed by the response and recovery actions from the viewpoint of the <<Indiana City>>’s stakeholders.

The plan is not intended to provide a technical guide on resolving an incident but instead to define an operational cyber response for <<Indiana City>>.

## SCOPE

With <<Lead Party>> as the lead coordinating Department for <<Indiana City>>’s cybersecurity efforts, this plan was developed to provide guidance for a cyber incident. The plan also provides a playbook on the incident management aspects of responding to and recovering from an incident, including the parties responsible, accountable, consulted, and informed over the course of the response.

While <<Lead Party>> is tasked with the program oversight, several groups and individuals play vital roles in the program’s execution, as outlined in this plan. These include:

* Elected Officials – responsible for controlling, maintaining, and supervising <<Indiana City>> property, determining appointees to the Information Technology Board, auditing and authorizing claims, receiving bids, and assigning contracts, budgets, and oversight of grants.
* Information Technology Board – oversight of the IT infrastructure for the <<Indiana City>> and the staffing of the response and recovery team during a cybersecurity incident.
* <<Lead Party>> – oversight of the cybersecurity program, grants for the program, and management of the Emergency Operations Center during an incident.
* <<Indiana City>> Cyber Incident Response Team – the collective group of selected individuals from the Elected Officials, Information Technology Board, <<Lead Party>>, <<Indiana City>> Information Technology provider, and the <<Indiana City>> Public Information Officer/Joint Information System to execute this plan.
* <<Indiana City>> Emergency Operations Center (EOC) – point of contact for efforts during a cyber incident staffed by members of the Cyber Incident Response Team.
* <<Indiana City>> Information Technology provider – <<Indiana City>> Department or subcontracted private sector partner accountable for daily operations and preventative cybersecurity efforts and controls.
* Cybersecurity services providers – subcontracted private sector partners accountable for training and response efforts.
* <<Indiana City>> Public Information Officer/Joint Information System – single point of contact for all information management for a cyber incident.

## SITUATION OVERVIEW

According to the National Associate of State Chief Information Officers, representing the Chief Information Officers of the States, the top enterprise risk for 2022 is cybersecurity, ahead of technology, operational, and external risks. The risks to data theft, insider threats, where users unknowingly open a vulnerability, dependencies on third-party practices as outsourcing increases, determining what constitutes “due care” or “reasonable” cyber programs and policies, and then addressing ransomware and identify theft have created focused cyber teams.

Cybersecurity is a critical leadership issue. New regulations and reporting requirements make cybersecurity risk oversight a challenge. Leadership will continue to seek assurances from their information technology and cybersecurity teams that their cyber risk strategies will reduce the risk of attacks and limit financial and operational impacts.

Cybercrime is a costly business at an estimated $6 trillion annually, which would qualify it as the world’s third-largest economy after the U.S. and China. Attackers can also be driven by political, ethical, or social incentives. Emerging privacy laws can mean significant fines for organizations. There are also non-financial costs to be considered, like reputational damage.

And cybercriminals don’t have to steal data to make money – they can just stop you from using it. Ransomware is the most prevalent variety of malware. It’s easy to deploy and can be very effective – off-the-shelf toolkits allow any amateur to create and deploy ransomware in a matter of minutes.

The time it takes cybercriminals to compromise a system is often just a matter of minutes – or even seconds. They don’t need much time to extract valuable data - they usually have much more than they need as it typically takes organizations weeks or months to discover a breach.

Once impacted, such as with a ransomware attack, the average interruption time - which is defined as not at 100% capacity - as of the third quarter of 2021 was 22 days, according to statista.com. The costs associated with downtime, people hours, device costs, network costs, ransom paid, etc., was $1.85 million per organization in 2021, according to Sophos, a leading provider of cyber prevention software.

What are the major types of cyber-attacks? The following is a breakdown of the most common ones:

* ***Ransomware*** – one of the fastest-growing forms of cyber-attack and has been behind a number of high-profile breaches. It is a type of malware (malicious software) that encrypts a victim’s files and demands a payment to release them. However, paying the ransom does not guarantee the recovery of all encrypted data.
* ***Phishing*** – is an attempt to access sensitive information such as passwords and bank information by posing as a trusted individual. Phishing is done via electronic communication, most commonly by email, and can inflict enormous damage on organizations.
* ***DDoS Attack*** – a distributed denial-of-service attack is a malicious attempt to disrupt normal web traffic and take a site offline. This type of attack is done by flooding a system, server, or network with more access requests than it can handle.
* ***Viruses*** – are a malicious code loaded onto a computer without the user’s knowledge. It can replicate itself and spread to other computers by attaching itself to another computer file.
* ***Trojans*** – are a type of malware that disguises itself as legitimate software, such as virus removal programs, but performs malicious activity when executed.
* ***Zero-day Attack*** – takes advantage of outdated (unpatched) software and the opportunities for criminal hackers to exploit vulnerabilities to bring entire systems down. A zero-day exploit can occur when a vulnerability is made public before the developer has rolled out a patch or solution.
* ***Spyware/adware*** – can be installed on your computer without your knowledge when you open attachments, click malicious links, or download infected software. It then monitors your computer activity and collects personal information.
* ***Worms*** – are similar to viruses in that they are self-replicating, but they do not need to attach themselves to a program. They continually look for vulnerabilities and report any weaknesses they find to their creator.

# INCIDENT RESPONSE

## Team Organization

The concept of operations for <<Indiana City>> cyber response includes multiple teams, each with its own set of responsibilities. The following outlines each of the teams and their primary roles and responsibilities.

### Cyber Incident Response Team

The <<Indiana City>> Cyber Incident Response Team forms the ownership of the incident response and provides the management directives on the actions taken by <<Indiana City>>. Based on the severity of the incident and the scale of the response, this team includes members from elected officials, <<Lead Party>> Department, The city technology provider, <<Indiana City>> offices, Risk Management, the <<Indiana City>> Public Information Officer/Joint Information System, and the <<Indiana City>>’s legal representatives.

With <<Lead Party>> as the lead coordinating Department for the Cyber Incident Response Team, the team falls under the guidance of the <<Indiana City>>’s Emergency Operations Plan and its provisions and would operate from the <<Indiana City>> Emergency Operations Center.

**Full Activation Organization Chart**

The Cyber Incident Response Team is responsible over the lifecycle of a cyber incident to:

* Serve as the primary recipient of the cyber incident status reports, including all incident assessments, communications, forensics, mitigation, eradication, and recovery efforts.
* Determination of the impact of the incident.
* Determination of staffing of active teams for the <<Indiana City>>.
* Lead and coordinate activities across the active teams.
* Direct operational planning as defined by the <<Indiana City>>’s EOC battle rhythm and/or ICS operational planning guidance.
* Review and approve internal and external messages.

**Cyber Incident Response Team Roles:**

***Policy Group Representative*** – provides strategic direction and coordination of the Cyber Incident Response Team. The representative provides the final decision authority during an event.

* Key Activities:
  + The final decision on the incident severity level.
  + Provide authority to staff the Cyber Incident Response Team from <<Indiana City>> government members.
  + Ability to authorize activities and response actions.
  + Review and approve communications releases.
  + Act as liaison to elected officials and the Policy Group.

***EOC Manager***

* Key Activities:
  + Manage the operations of the EOC.
  + Serve as the point of contact for the initial assessment of an event.
  + Conduct initial activation and meeting of the Cyber Incident Response Team.

***Administrative Support***

* Key Activities:
  + Assist with the activation of the EOC.
  + Assist with communications with response team members on activation and status updates.
  + Assist with logistical needs for the EOC, such as office supplies, printing, food, and facility needs.
  + Assist with information management via collaboration sites, generating and distributing situation reports, and maintaining documentation.
  + Provide as-needed assistance to support EOC operations.

***External Liaison***

* Key Activities:
  + Provide the point of contact for external parties.
  + Coordinate external parties’ information within the Cyber Incident Response Team.
  + Provide the assignment of roles if included in the Cyber Incident Response Team.

***Threat Response***

* Key Activities:
  + The city technology provider representative is the lead representative of the threat response efforts. Guide the technical impact and how it corresponds with the ability to continue <<Indiana City>> operations.
  + Information Technology partners – technical response efforts.
  + Cybersecurity partners – cyber response efforts.
  + City Law Enforcement – leads the law enforcement efforts for <<Indiana City>> and is the liaison to external law enforcement agencies.

***Operational Response***

* Key Activities:
  + The <<Lead Party>> Department will provide guidance and input on the continuity of operations efforts and considerations for <<Indiana City>> agencies.
* Comprised of representatives from impacted <<Indiana City>> agencies.

***Legal***

* Key Activities:
  + decision authority for interpreting legal and regulatory requirements.

***Public Information***

* Key Activities:
  + provides strategy and communications efforts for all internal and external messages.

***Planning and Logistics***

* Key Activities:
  + *Situational Awareness* - Collecting, evaluating, disseminating, and using information about the incident and the status of resources.
  + Participate in the operational planning process and meetings.
  + Conduct situation updates at meetings and briefings.
  + Collect and organize incident files, information, forms, incident action plans, information releases, and reports.
  + Identify service and support requirements for planned and expected operations.
  + Coordinate and process requests for additional resources.

\*\*\*\* County Emergency Management may fulfill this role and will need to be engaged to request State resources.

***Finance***

* Key Activities:
  + Human Resources – assisting with internal policy decisions and internal communications.
  + Monitor and coordinate funding from multiple resources.
  + Provide financial and cost analysis information as requested.

Additional teams that operate outside of the ***Cyber Incident Response Team*** to support the incident include:

### Policy Group

The Policy Group focuses on the overall strategy for the response (beyond the strategy developed by the Cyber Incident Response Team), the overall response priorities, and policy review and decisions. The Cyber Incident Response Team implements decisions made by the Policy Group. They meet to develop emergency policies and then, as required by the disaster situation, discuss the economic, political, legal, and social implications of both the threat and the response to determine the best general approach to the incident. The Policy Group may elect to remain at the Emergency Operations Center (EOC) to observe but may also be available by pager, telephone, or email.

### Communications

The Public Information Officer is responsible for communicating information to the public during the incident. Their communication (written or spoken) will be the official and only information provided by the Policy Group. The <<Indiana City>>’s Emergency Operations Plan ensures that sufficient local assets are deployed to the field during incidents requiring a coordinated local response to provide accurate, coordinated, and timely information to affected audiences, including governments, media, the private sector, and the local populace.

The staffing of the Public Information Office should consider the following assignments:

* Public Information Officer (PIO) / Lead Public Information Officer
* Assistant PIO (APIO) for Information Gathering – Incident information, status board, media monitoring, rumor control.
* APIO for Information Products – writer, imagery, website.
* APIO for Media Relations – media inquiries, selecting and preparing speakers, conducting news briefings, coordination of release of information to media.
* APIO for Community Relations – determine information needs of the community, develop and coordinate community outreach programs, conduct community meetings, outreach materials, volunteer opportunities, and all social media aspects.

### Information Technology and Cyber Response

The threat response is performed by the city’s technology provider and the internal and external resources that support <<Indiana City>>’s infrastructure and cybersecurity efforts. The city technology provider leadership will manage these resources.

## Cyber Incident Severity Levels

The classifications below guide the active response teams in evaluating and assessing an event based on the actual or potential impact on <<Indiana City>>. This allows for an objective reading of facts and circumstances based on a uniform set of criteria that can be compared against a severity level. The conditions are guidelines for classifying an incident. They are meant to supplement the real-world assessment of the overall cyber threat conditions and the impact on <<Indiana City>> and its citizens.

* + ***Local Incident*** – condition will be contained without significant impact on <<Indiana City>> operations, no legal or compliance concerns, and the city technology provider can resolve the issue and update the <<Indiana City>>’s Cyber Incident Response Team on return to normal operations.
  + ***Minor Incident*** - condition will be contained with minor impact to <<Indiana City>> operations (hours up to days), potential legal or compliance concerns, the city technology provider and cybersecurity resources will be actively engaged. This will require the activation of the <<Indiana City>> Cyber Incident Response Team to provide resources to help support and coordinate the response.
  + ***Major Incident*** – containment of the condition is uncertain with significant impact on <<Indiana City>> operations (days to weeks), identified legal or compliance concerns due to loss or damage to information or ability to provide <<Indiana City>> services, the city technology provider and cybersecurity resources will be actively engaged. This will require the activation of the <<Indiana City>> Cyber Incident Response Team to oversee the response.

The following evaluation National Institute of Standards and Technology (NIST) guidelines are provided to help quantify the effect of an incident based on situational awareness.

**Functional Impact Categories**

|  |  |
| --- | --- |
| **Category** | **Definition** |
| None | No effect to the organization’s ability to provide all services to all users |
| Low | Minimal effect: 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 Categories**

|  |  |
| --- | --- |
| **Category** | **Definition** |
| None | No information was exfiltrated, changed, deleted, or otherwise compromised |
| Low | Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated |
| Medium | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated |
| High | Sensitive or proprietary information was changed or deleted |

**Recoverability Effort Categories**

|  |  |
| --- | --- |
| **Category** | **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 and posted publicly); launch an investigation |

## Cyber Incident Lifecycle Overview

Taken from the guidance provided by NIST in its publication “Framework for Improving Critical Infrastructure Cybersecurity”, a summary of the key events during the incident include:

* Detection:
  + Detected events are analyzed to understand attack targets and methods.
  + The impact of events is determined.
  + Incident alert thresholds are established.
* Response:
  + Communications:
    - Coordination with stakeholders occurs consistent with response plans.
  + Analyze:
    - The impact of the incident is understood.
    - Forensics are performed.
    - Incidents are categorized consistent with response plans.
    - Processes are established to receive, analyze, and respond to vulnerabilities.
  + Mitigation:
    - Incidents are contained.
    - Incidents are mitigated.
  + Recovery:
    - Eradication of the threat is conducted.
    - Recovery of impacted systems.
    - Restoration activities are coordinated with internal and external parties, and public relations are managed.
    - Recovery plans incorporate lessons learned.

## Detection of a Cyber Incident

This section covers the recognition of an incident and those areas that might first identify an issue. Then, the assessment and escalation procedures are outlined based on the validation of a cyber incident.

### Recognition of a potential incident

Many different types of events may occur that can trigger a cybersecurity incident response. A sample of the triggering events that would cause the activation of the response plan include the loss, theft, unauthorized disclosure, or alteration of:

* Information or Data –protected information by State statutes or classified as personal or confidential information.
* Computers or supporting devices – servers, data storage devices.
* Applications or externally facing websites, or the internet and its infrastructure.

The recognition of an event may initiate from the <<Indiana City>>’s Help Desk provider and the monitoring mechanisms they provide. It could also originate from one of <<Indiana City>>’s employees, third parties or providers, website users, or an advisory from law enforcement officials.

However, once a potential issue is identified, it must be brought to the attention of the <<Indiana City>> Cyber Incident Response Team for assessment and possible escalation. Once an issue is recognized, the following details how information should flow:

1. The potential issue is identified.
2. Known impacts are documented, and the ability to manage the incident is determined.
3. Initial assessment by the city technology provider, level of impact determined.
4. If there is minimal impact or no legal or compliance concerns, the city technology provider addresses the issue and provides a report to the <<Indiana City>>’s Cyber Incident Response Team.
5. Otherwise, as the lead coordinating Department for the <<Indiana City>> Cyber Incident Response Team, <<Lead Party>> would be notified to review the incident and the potential severity of the event. Based on the incident severity, <<Lead Party>> will either partially or fully activate the <<Indiana City>> Cyber Incident Response Team to address the event.

## Cyber Incident Response Tasks RESPONSE – START HERE!

### Upon Detection and Notification to the Cyber Incident Response Team

The following checklist guides the Cyber Incident Response Team’s initial leader during the activation of response operations for an event. Some steps may not be required based on the event, and others may need to be added. Once notified of an event, your ability to act quickly will reduce an incident’s potential impact and recovery time.

* Cyber Incident Response Team initial leader to obtain an initial briefing on the situation from the city technology provider, only look for FACTS.
* Assess the situation:
* Determine if the incident creates any life safety issues, such as with 911. Ensure that all local authorities that should be notified have been notified.
* Assess the impact on <<Indiana City>> operations and determine the magnitude of the potential impact.
* Determine your team - who will be required to assess the event’s impacts further, mitigate the risks identified, or manage the response to the event. Determine the staffing required to meet initial objectives and utilize emergency notification, email, or phone calls to activate them.
* Set a team meeting - Determine the time and location of the first meeting – the 1st meeting could be a conference call or in a command center location based on availability.
* Brief the Team – Initial Meeting should include:
* Select a Scribe to document the meeting. Use the ‘Status Report Template’ – as it should provide ideas on what intelligence to gather.
* Review the facts about the event – assign who is responsible for obtaining additional factual information and maintaining situational awareness.
* Determine incident objectives and assign initial tasks.
* Determine if shifts will need to be delegated and the time frame for staff turnover (see Staffing Considerations below).
* Determine where you will set up the command center if it has not already been set up.
* Determine regular status meeting cadence/schedule next meeting.
* Determine what additional internal and external teams need to be notified or activated.
* Work with the assigned Public Information Officer to review the message approval process and confirm capabilities to develop messages designed for internal and external audiences. See Sections IX and X for contact lists.
* If warranted, ensure the <<Indiana City>> officials are briefed on the situation and determine a cadence of updates.
* Identify the city technology provider’s internal and external resources currently active and the strategies and tactics underway to contain and mitigate the incident. Determine best-case and worst-case scenarios on impacted areas and additional required resources.
* Build a response roadmap, including the immediate Cyber Incident Response Team-specific actions at each response phase.
* Determine what external reporting will be required and when, including legal, insurance, and compliance requirements.
* Determine what public information must be developed and shared and the timeline.
* Identify potential financial costs and approval processes for funding.
* Document the incident action plan from the initial meeting and post.

### Mitigation and Recovery

The following provides the operational guidance during the mitigation and recovery phase of the response. These activities are broken into two categories: Threat Response and Operational Response.

*Threat Response* includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It also includes conducting criminal investigations and other actions to counter malicious cyber activity. The <<Indiana City>>’s city technology provider, cybersecurity internal and external resources, and local law enforcement conduct the threat response.

*Operational Response* includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact on systems and/or data, strengthening, recovering, and restoring <<Indiana City>> services, identifying other entities at risk, and assessing the potential risk to the broader community.

#### Threat Response

The <<Indiana City>>’s city technology provider and cybersecurity internal and external resources conduct the threat response actions based on the review and approval from the <<Indiana City>> Cyber Incident Response Team. The following is a guideline of the procedures to be followed over the Mitigation and Recovery phases of the response.

Mitigation:

* Confirm containment measures are currently being undertaken. Review authority that is required to execute each as needed.
* Confirm identification of root cause and assess impacts.
* Review the type of data affected and operational impacts.
* Review investigatory and regulatory actions underway.
* Review insurance carrier support actions and claim procedures.
* Identify internal and external communication requirements.
* Confirm and authorize mitigation strategies as appropriate.
* Determine post-containment assessment activities required.

Recovery:

* Review post-containment impact assessment.
* Confirm eradication completion.
* Review data and systems impacted and approve recovery strategies.
* Prepare to brief <<Indiana City>> operations on the recovery strategies to aid in developing the reconstitution of operations.
* Review insurance carrier requirements for the financial impact.
* Identify internal and external communications requirements.
* Monitor restoration of <<Indiana City>> services for completion.

#### Operational Response

Review the impacted <<Indiana City>> operations and their critical functions and recovery priorities with impacted departments to formulate an operational response. This follows the flow of an abbreviated Continuity of Operations departmental assessment, which can be found in the appendix.

Mitigation:

* From the initial assessment conducted, ensure an impact timeline has been detailed that identifies:
  + the applications or services that have been interrupted,
  + the departmental processes that have been impacted and their criticality level,
  + any time-sensitive work in progress that needs to be accounted for.
* For the time-sensitive business functions that are at risk of not being completed as required, such as payroll, determine:
  + potential solutions and resources needed for manual workarounds,
  + assign required tasks, and monitor the progress of resolution.
* Determine any potentially lost information and the requirements to capture ongoing work in progress.
* Determine and document the impact of the department’s abilities to support upstream and downstream business processes and external parties.
* Determine access to any information sources that alternatively may be used to support ongoing business operations.
* Determine and document policies for manual workarounds until services are restored.
* Document the overall impact of the outage and the status of the impacted departments to support ongoing business operations.

Restoration:

* Work with the threat response resources to identify a most likely restoration process and the recovery point in time for information.
  + Determine requirements for the department(s) to resume operations with restored services, identify and input any lost information, and address input of the backlog of information.
  + Upon notification of the restoration of services, monitor the validation of systems and the point in time the data has been restored to. Update the resources and time required to bring the environment current. Monitor implementation of the restoration process.
* Establish a cadence for updates on the restoration process and its timing.
* Ensure that external parties are notified of any impacts they need to be aware of.

### Continued Operational Periods Planning (IAP)

The following provides the high-level cadence for ongoing additional operational planning based on ICS Operational Planning.

#### Conduct Planning and Logistics Meetings

Utilizing the following guidance, the Cyber Incident Response Team will review the ongoing impact of the incident, the response priorities, and any additional resources or activation of additional recovery strategies required to support the event.

* Review incident objectives and status reports and verify current tactics will continue to meet objectives. Identify gaps and determine additional tactics as required. Consider:
  + Current assessments of the damage or impacts.
  + Availability of alternative resources, equipment, and supplies.
  + Updated restoration times.
  + Impact of lost information.
* Review how the selected strategy(s) are being accomplished and whether they will continue to meet the incident objectives over the next operational period.
* Identify additional resources as needed.
* Prepare an updated situation report and update the Incident Action Plan QuickStart.

### Update Response and Recovery Recommendations

Provide recommendations on which additional strategies should be implemented, taking into account the results of the assessment process and any unique timing or business conditions that have changed (such as during month-end heavy business volume).

* Review and update threat and operational strategies considering:
* The areas affected by the incident.
* Pre-planned recovery timing objectives.
* Availability of required resources.
* Special timing circumstances such as the beginning of a day, during heavy flow volumes, or during month-end activities.
* Potential penalties, fines, or other adverse effects.
* Communication requirements.
* Contractual obligations.
* Update the restoration priority list as needed, considering the available resources and current business requirements.
* Review staffing for the Cyber Incident Response Team and determine requirements for ongoing operational periods.
* Update the Incident Action Plan Quick Start to reflect the updated strategies and tactics the Cyber Incident Response Team leadership approved. This form clearly communicates the current status and the incident recovery objectives to interested parties, elected officials, and the response teams.

## Demobilization

As the impacted <<Indiana City>> operations return to normal operations, the Cyber Incident Response Team will need to provide oversight of the release of resources, ensure documentation is complete, and conduct an after-action review as required. By position, sample tasks include:

***EOC Manager***

* Key Activities:
  + Establishing the release priorities.
  + Review and approve the demobilization plan.
  + Review and approve all tentative release sheets.

***Administrative Support***

* Key Activities:
  + Assist with the deactivation of the EOC.
  + Assist with communications with response team members on deactivation and status updates.
  + Assist with re-purposing equipment such as office supplies.
  + Assist with information management via collaboration sites, collection of situation reports, and maintaining incident documentation.
  + Provide as-needed assistance to support EOC operations.

***External Liaison***

* Key Activities:
  + Provide the point of contact for external parties for their demobilization.

***Operational and Threat Response***

* Key Activities:
  + Document lessons learned over the course of the response.
  + Ensure all documentation and financial receipts are complete.

***Legal***

* Key Activities:
  + Document pending litigation surviving the activation.
  + Provide necessary close-out documentation.
  + Document lessons learned over the course of the response.

***Public Information***

* Key Activities:
  + Provide the necessary communications around deactivation.
  + Document lessons learned throughout the response.

***Planning and Logistics***

* Key Activities:
  + Ensure all documentation is complete and recorded, including incident files, information, forms, incident action plans, information releases, and reports.
  + Ensure personnel and vendor time records are up to date.
  + Manage incident resources as they are redistributed.
  + Document lessons learned throughout the incident.

***Finance***

* Key Activities:
  + Finalize documentation from funding resources.
  + Prepare a financial summary of event expenses.
  + Document lessons learned throughout the incident.

# Cyber Incident Response Team Assignment Form

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CYBER INCIDENT RESPONSE TEAM ORGANIZATION ASSIGNMENT FORM** | | | | | |
| **Incident Name** | | | | **Date / Time** | |
|  | | | | | |
| **CYBER INCIDENT RESPONSE TEAM STAFFING** | | | | | |
| **Team Role** | **Name** | **Location** | **Primary Contact Information** | | **Secondary Contact Information** |
| Policy Group Representative |  |  |  | |  |
| EOC Manager |  |  |  | |  |
| Public Information |  |  |  | |  |
| External Liaison |  |  |  | |  |
| Administrative Support |  |  |  | |
| Threat Response |  |  |  | |  |
| Operation Response |  |  |  | |  |
| Planning and Logistics |  |  |  | |  |
| Finance |  |  |  | |  |
| Legal |  |  |  | |  |
| IT Resources |  |  |  | |  |
| Cyber Resources |  |  |  | |  |
| Law Enforcement |  |  |  | |  |
| <<Indiana City>> Departments |  |  |  | |  |
| Human Resources |  |  |  | |  |
| Situational Awareness |  |  |  | |  |

# Cyber Incident Reporting Guidance

The following provides guidance on reporting a cyber incident and the regulatory guidance identified and applicable at the time of this document's last update. Additional regulations or guidance are under continual development, revision, and updates; therefore, this section should not be considered all-inclusive at the time of an event and should be reviewed with the agencies as they are notified and become engaged in the response.

## Definitions – Cyber Emergency vs. Cyber Incident, IOT

The State of Indiana defines a **cyber emergency** as any actual, imminent, or potential incident that will adversely affect public health, safety, or security, the environment, or economic prosperity on a level materially significant to the State of Indiana or its operations that requires a coordinated state response.

The State of Indiana defines a **cyber incident** as it is described in the [Presidential Policy Directive 41](https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident), which is “an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon.”

*If you have cyber insurance, it is important to note that the following steps should be verified by the response procedures with you carrier.*

## ****State level event Reporting****

All local government/public-sector entities are required to report incidents such as ransomware, software vulnerability exploitations, denial-of-service attacks and more to the Indiana Office of Technology IN-ISAC within 48 hours of the incident. To learn more, visit <https://www.in.gov/cybersecurity/in-isac/cyber-incident-reporting-law/>

* **Sign up to be a point of contact for your organization:** <https://public.govdelivery.com/accounts/INIOT/signup/26666>
* **Report a cybersecurity incident:** <https://soi.formstack.com/forms/incident_reporting_form>

## [Law](https://www.in.gov/cybersecurity/report-a-cyber-crime/#null) enforcement event reporting

Law enforcement performs an essential role in achieving the nation’s and state’s cybersecurity objectives by investigating, apprehending, and prosecuting those responsible for a wide range of cybercrimes.

**If you are reporting a cybercrime, contact one of the following law enforcement agencies right away.**

* ***FBI - Internet Crime Complaint Center (IC3)***

The [FBI Internet Crime Complaint Center's (IC3)](https://www.ic3.gov/default.aspx) mission is to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. The IC3 gives the victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations.

* + [FBI Cyber](https://www.fbi.gov/investigate/cyber) - The FBI is the lead federal agency for investigating cyberattacks and intrusions. To learn more about what you can do to protect yourself against various forms of cybercrimes, FBI Cyber offers a great deal of information and resources including:
    - [Partnering with the FBI](https://www.in.gov/cybersecurity/files/Partnering_with_the_FBI.pdf)
    - [Benefits of Reporting a Cyber Incident to the FBI](https://www.in.gov/cybersecurity/files/QuickBytes_-_PocketGuide.pdf)
* ***Indiana State Police (ISP)***ISP’s [Cybercrime & Investigative Technologies Section](http://www.in.gov/isp/3234.htm) has detectives who specialize in conducting cybercrime investigations. Call (317) 232-8248.
* ***Immediate Threat to Public Safety***  
  If there is an immediate threat to public health or safety, the public should always call 911.

**Additional Reporting to Consider:**

* ***USDHS Cybersecurity & Infrastructure Security Agency***

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to [report@cisa.gov](mailto:report@cisa.gov) or [(888) 282-0870](tel:888-282-0870). To learn more, visit [www.cisa.gov/report](http://www.cisa.gov/report).

* ***Indiana Attorney General***

Indiana’s security breach notification statute requires organizations to provide Indiana residents with the right to know when a security breach has resulted in the exposure of their personal information. For more information and to report a security breach, click [here](https://www.in.gov/attorneygeneral/3037.htm).

* ***Regulators***

If you are an organization that is regulated, you may be required to report cybercrimes to other state or federal agencies.

* ***Federal Government***

This fact sheet, [Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government](https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf), further explains when, what, and how to report a cybercrime to a number of federal agencies.

## [Additional](https://www.in.gov/cybersecurity/report-a-cyber-crime/#null) Resources during a Cyber Event

The following resources, with links, are provided for additional guidance, information, and resources during a cyber event:

* [CISA Shields Up – Cyber Guidance](https://www.cisa.gov/shields-up)
* [MS-ISAC Security Primer on Ransomware](https://www.cisecurity.org/white-papers/ms-isac-security-primer-ransomware)
* [CISA Stop Ransomware Guide](https://www.us-cert.gov/Ransomware)
* [NGA Disruption Response Planning Memo](https://www.nga.org/wp-content/uploads/2019/04/IssueBrief_MG.pdf)
* **National Institute of Standards and Technology (NIST)**  
  NIST’s [Computer Security Incident Handling Guide](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final) assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.
* **Ready.gov**  
  [Ready.gov](https://www.ready.gov/cybersecurity) is a national public service campaign designed to educate and empower the American people to prepare for, respond to, and mitigate emergencies, including cybersecurity.

## [information](https://www.in.gov/cybersecurity/report-a-cyber-crime/#null) sharing

If you are a victim of a cybercrime, it is important to share such information with other organizations in order to protect critical infrastructure, the state of Indiana, and our nation. Learn more about <https://www.in.gov/cybersecurity/government/cyber-threat-sharing>.

# Indiana Regulatory Codes and Industry Standards

## Indiana Codes

The following is an overview and then reference to [Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.](http://iga.in.gov/legislative/laws/2018/ic/titles/004)

* Enacted in 2005, Indiana’s data breach notification law requires entities that own or license computerized personal information to notify Indiana residents of any unauthorized acquisition of their unencrypted or unredacted personal information if it could result in identity theft or fraud.
* Notice shall be made without unreasonable delay. Data base owners must also disclose the breach to the Attorney General.
* If more than 1,000 individuals must be notified of a breach, breached entities must also inform all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC Section 1681a(p).
* Substitute notice is permitted in specific circumstances and notification may be delayed for law enforcement purposes.
* Breached third parties must notify the relevant data owners or licensees.
* Entities which maintain their own notification procedures as part of an information security policy consistent with state law are deemed to comply with the notification requirements of this law if the entity makes notifications in accordance with its policies.
* Entities in compliance with [HIPAA](https://www.itgovernanceusa.com/hipaa), the [GLBA](https://www.itgovernanceusa.com/cyber-security-regulations#6), the USA PATRIOT Act, and other named laws are deemed to comply with this law.
* Knowingly or intentionally failing to comply with database maintenance obligations is actionable only by the state Attorney General with penalties up to $150,000 per violation.

|  |  |
| --- | --- |
| **IC 4-1-11** | **Chapter 11. Notice of Security Breach** |

|  |  |
| --- | --- |
| [4-1-11-1](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-1) | Applicability |
| [4-1-11-2](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-2) | "Breach of the security of the system" |
| [4-1-11-3](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-3) | "Personal information" |
| [4-1-11-4](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-4) | "State agency" |
| [4-1-11-5](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-5) | Disclosures of security breach |
| [4-1-11-6](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-6) | Notification to third party owner of security breach |
| [4-1-11-7](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-7) | Time requirement for notification |
| [4-1-11-8](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-8) | Form of notification |
| [4-1-11-9](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-9) | Alternate form of notification |
| [4-1-11-10](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-11-10) | Notification to consumer reporting agencies |

|  |  |
| --- | --- |
| **IC 4-1-11-1** | **Applicability** |

This chapter applies after June 30, 2006.

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-2** | **"Breach of the security of the system"** |

(a) As used in this chapter, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency.

(b) The term does not include the following:

(1) Good faith acquisition of personal information by an agency or employee of the agency for purposes of the agency, if the personal information is not used or subject to further unauthorized disclosure.

(2) Unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed.

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-3** | **"Personal information"** |

(a) As used in this chapter, "personal information" means:

(1) an individual's:

(A) first name and last name; or

(B) first initial and last name; and

(2) at least one (1) of the following data elements:

(A) Social Security number.

(B) Driver's license number or identification card number.

(C) Account number, credit card number, debit card number, security code, access code, or password of an individual's financial account.

(b) The term does not include the following:

(1) The last four (4) digits of an individual's Social Security number.

(2) Publicly available information that is lawfully made available to the public from records of a federal agency or local agency.

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-4** | **"State agency"** |

As used in this section "state agency" has the meaning set forth in [IC 4-1-10-2](http://iga.in.gov/legislative/laws/2018/ic/titles/004#4-1-10-2).

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-5** | **Disclosures of security breach** |

(a) Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

(b) The disclosure of a breach of the security of the system shall be made:

(1) without unreasonable delay; and

(2) consistent with:

(A) the legitimate needs of law enforcement, as described in section 7 of this chapter; and

(B) any measures necessary to:

(i) determine the scope of the breach; and

(ii) restore the reasonable integrity of the data system.

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-6** | **Notification to third party owner of security breach** |

(a) This section applies to a state agency that maintains computerized data that includes personal information that the state agency does not own.

(b) If personal information was or is reasonably believed to have been acquired by an unauthorized person, the state agency shall notify the owner or licensee of the information of a breach of the security of the system immediately following discovery. The agency shall provide the notice to state residents as required under section 5 of this chapter.

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-7** | **Time requirement for notification** |

The notification required by this chapter:

(1) may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; and

(2) shall be made after the law enforcement agency determines that it will not compromise the investigation.

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-8** | **Form of notification** |

Except as provided in section 9 of this chapter, a state agency may provide the notice required under this chapter:

(1) in writing; or

(2) by electronic mail, if the individual has provided the state agency with the individual's electronic mail address.

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-9** | **Alternate form of notification** |

(a) This section applies if a state agency demonstrates that:

(1) the cost of providing the notice required under this chapter is at least two hundred fifty thousand dollars ($250,000);

(2) the number of persons to be notified is at least five hundred thousand (500,000); or

(3) the agency does not have sufficient contact information;

the state agency may use an alternate form of notice set forth in subsection (b).

(b) A state agency may provide the following alternate forms of notice if authorized by subsection (a):

(1) Conspicuous posting of the notice on the state agency's web site if the state agency maintains a web site.

(2) Notification to major statewide media.

*As added by P.L.91-2005, SEC.2.*

|  |  |
| --- | --- |
| **IC 4-1-11-10** | **Notification to consumer reporting agencies** |

If a state agency is required to provide notice under this chapter to more than one thousand (1,000) individuals, the state agency shall notify without unreasonable delay all consumer reporting agencies (as defined in 15 U.S.C. 1681a) of the distribution and content of the notice.

*As added by P.L.91-2005, SEC.2. Amended by P.L.1-2006, SEC.7.*

|  |  |
| --- | --- |
| **Section 24-4.9-3-1** | **Disclosure of breach** |

**(a)** Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of data, the database owner shall disclose the breach to an Indiana resident whose:

**(1)** unencrypted personal information was or may have been acquired by an unauthorized person; or

**(2)** encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.

**(b)** A database owner required to make a disclosure under subsection (a) to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.

**(c)** If a database owner makes a disclosure described in subsection (a), the database owner shall also disclose the breach to the attorney general.

As added by P.L. 125-2006, SEC.6. Amended by P.L. 137-2009, SEC.4.

|  |  |
| --- | --- |
| **Section 24-4.9-3-2** | **Notification of database owner** |

A person that maintains computerized data but that is not a database owner shall notify the database owner if the person discovers that personal information was or may have been acquired by an unauthorized person.

As added by P.L. 125-2006, SEC.6.

|  |  |
| --- | --- |
| **Section 24-4.9-3-3** | **Delay of disclosure or notification** |

**(a)** A person required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay, but not more than forty-five (45) days after the discovery of the breach. For purposes of this section, a delay is reasonable if the delay is:

**(1)** necessary to restore the integrity of the computer system;

**(2)** necessary to discover the scope of the breach; or

**(3)** in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will:

**(A)** impede a criminal or civil investigation; or

**(B)** jeopardize national security.

**(b)** A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after:

**(1)** delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or

**(2)** the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.

Amended by P.L. 171-2022,SEC. 1, eff. 7/1/2022.As added by P.L. 125-2006, SEC.6.

|  |  |
| --- | --- |
| **Section 24-4.9-3-3.5** | **Duties of a database owner; exceptions; health records; enforcement powers** |

**(a)** Except as provided in subsection (b), this section does not apply to a database owner that maintains its own data security procedures as part of an information privacy, security policy, or compliance plan under:

**(1)** the federal USA PATRIOT Act ( P.L. 107-56 );

**(2)** Executive Order 13224;

**(3)** the federal Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.);

**(4)** the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

**(5)** the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or

**(6)** the federal Health Insurance Portability and Accountability Act (HIPAA) ( P.L. 104-191 ); if the database owner's information privacy, security policy, or compliance plan requires the database owner to maintain reasonable procedures to protect and safeguard from unlawful use or disclosure personal information of Indiana residents that is collected or maintained by the database owner and the database owner complies with the database owner's information privacy, security policy, or compliance plan.

**(b)** This section applies to a current or former health care provider (as defined by IC 4-6-14-2) who is a database owner or former database owner:

**(1)** to which an exemption under subsection (a)(6) applies or applied; and

**(2)** whose information privacy, security policy, or compliance plan:

**(A)** does not require the database owner or former database owner to maintain and implement reasonable procedures; or

**(B)** is not implemented by the database owner or former database owner; to ensure that the personal information described in subsection (a), including health records (as defined by IC 4-6-14-2.5) , is protected and safeguarded from unlawful use or disclosure after the database owner or former database owner ceases to be a covered entity under the federal Health Insurance Portability and Accountability Act ( P.L. 104-191 ).

**(c)** A database owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the database owner.

**(d)** A data base owner shall not dispose of or abandon records or documents containing unencrypted and unredacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the personal information illegible or unusable.

**(e)** A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act that is actionable only by the attorney general under this section.

**(f)** The attorney general may bring an action under this section to obtain any or all of the following:

**(1)** An injunction to enjoin further violations of this section.

**(2)** A civil penalty of not more than five thousand dollars ($5,000) per deceptive act.

**(3)** The attorney general's reasonable costs in:

**(A)** the investigation of the deceptive act; and

**(B)** maintaining the action.

**(g)** A failure to comply with subsection (c) or (d) in connection with related acts or omissions constitutes one (1) deceptive act.

Amended by P.L. 76-2017,SEC. 4, eff. 7/1/2017.As added by P.L. 137-2009, SEC.5.

|  |  |
| --- | --- |
| **Section 24-4.9-3-4** | **Method of disclosure; exceptions** |

**(a)** Except as provided in subsection (b), a database owner required to make a disclosure under this chapter shall make the disclosure using one (1) of the following methods:

**(1)** Mail.

**(2)** Telephone.

**(3)** Facsimile (fax).

**(4)** Electronic mail, if the database owner has the electronic mail address of the affected Indiana resident.

**(b)** If a database owner required to make a disclosure under this chapter is required to make the disclosure to more than five hundred thousand (500,000) Indiana residents, or if the database owner required to make a disclosure under this chapter determines that the cost of the disclosure will be more than two hundred fifty thousand dollars ($250,000), the database owner required to make a disclosure under this chapter may elect to make the disclosure by using both of the following methods:

**(1)** Conspicuous posting of the notice on the website of the database owner, if the database owner maintains a website.

**(2)** Notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.

**(c)** A database owner that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate disclosure under this chapter if the database owner's information privacy policy or security policy is at least as stringent as the disclosure requirements described in:

**(1)** sections 1 through 4(b) of this chapter;

**(2)** subsection (d); or

**(3)** subsection (e).

**(d)** A database owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under:

**(1)** the federal USA PATRIOT Act ( P.L. 107-56 );

**(2)** Executive Order 13224;

**(3)** the federal Driver's Privacy Protection Act (18 U.S.C. 2781 et seq.);

**(4)** the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

**(5)** the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or

**(6)** the federal Health Insurance Portability and Accountability Act (HIPAA) ( P.L. 104-191 ); is not required to make a disclosure under this chapter if the database owner's information privacy, security policy, or compliance plan requires that Indiana residents be notified of a breach of the security of data without unreasonable delay and the database owner complies with the database owner's information privacy, security policy, or compliance plan.

**(e)** A financial institution that complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, as applicable, is not required to make a disclosure under this chapter.

**(f)** A person required to make a disclosure under this chapter may elect to make all or part of the disclosure in accordance with subsection (a) even if the person could make the disclosure in accordance with subsection (b).

As added by P.L. 125-2006, SEC.6. Amended by P.L. 137-2009, SEC.6.

**INDIANA HOUSE ENROLLED ACT No. 1169**

In brief, House Bill 1169 Requires the Office of Technology to maintain a repository of cybersecurity incidents. Provides that a state agency and a political subdivision shall: (1) report any cybersecurity incident to the office without unreasonable delay and not later than two business days after discovery of the cybersecurity incident in a format prescribed by the chief information officer; and (2) provide the office with the name and contact information of any individual who will act as the primary reporter of a cybersecurity incident before September 1, 2021, and before September 1 of every year thereafter. Allows the Office of Technology to assist a state agency with certain issues concerning information technology. Provides that if requested by a political subdivision, the office may develop a list of third-party technology providers that work with the office. Requires a state educational institution to submit a quarterly analysis with certain conditions. Makes conforming changes.

The bill is available at:

<https://iga.in.gov/pdf-documents/122/2021/house/bills/HB1169/HB1169.04.ENRS.pdf>

## Industry Standards

Complying with the many state data breach notification laws can be complex. However, implementing and maintaining an Information Security Management System (ISMS) as laid out in the international information security management Standard ISO 27001 will help organizations achieve compliance with a host of related legislative and regulatory requirements.

The latest version of the Standard, [ISO 27001:2013](https://www.itgovernanceusa.com/shop/product/isoiec-27001-2013-iso-27001-standard-isms-requirements), is simple to follow and has been developed with business in mind. It presents a comprehensive and logical approach to developing, implementing, and managing an ISMS, and provides associated guidance for conducting risk assessments and applying the necessary risk treatments. In addition, [ISO 27001:2013](https://www.itgovernanceusa.com/shop/product/isoiec-27001-2013-iso-27001-standard-isms-requirements) has been developed in order to harmonize with other ISO standards, so the auditing process will be integrated and smooth, and will remove the need for multiple audits.

Furthermore, the additional external validation demonstrated by accredited registration to ISO 27001 will improve an organization’s cyber security posture while providing a higher level of confidence in customers and stakeholders, which is essential for securing certain global and government contracts.

IT Governance, a specialist in the field of information security, has created [ISO 27001 packaged solutions](https://www.itgovernanceusa.com/iso27001-solutions) to give US organizations online access to world-class expertise.

Each fixed-priced solution is a combination of products and services that will enable you to implement ISO 27001 at a speed and budget appropriate to your individual needs.

Alan Calder, Founder and Executive Chairman of IT Governance, commented: “If understood and implemented correctly, ISO 27001 can help to rationalize security expenditure and reduce the impact of cyber crime, while giving a business a competitive edge.”

NIST Special Publication 800-184, Guide for Cybersecurity Event Recovery, provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning. It also provides an example scenario that demonstrates guidance and information metrics that may be helpful improving resilience of information systems.

# Cyber Incident Continuity of Operations Assessment

At the time of an incident, it is essential for the <<Indiana City>> to assess the impact of the incident and implement available strategies to continue departmental operations while at the same time ensuring that information is maintained for entry once systems are restored. The following provides an assessment guideline for the impacted <<Indiana City>> operations:

* Please provide the operational impacts of this event on your department's critical functions, considering you may be without IT resources for days or weeks:
* Please provide the consequences and potential work required of restoring computer data to a point in time 30, 60, or 90 days in the past. All work between the restoration point and today would be lost.
* Please provide a restoration priority for the applications and IT services your department utilizes, such as we need email back first, payroll second, etc.
* Please provide to what degree your department can perform critical functions under these conditions.
* What resources or capabilities, if provided, would have the most significant impact on minimizing the effects of the event?

# Cyber Incident Response Team Members

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CYBER INCIDENT RESPONSE TEAM MEMBERS** | | | | |
| **Team Role** | **Name** | **Office Phone** | **Cell Phone** | **email** |
| Policy Group Representative - Primary |  |  |  |  |
| Policy Group Representative - Secondary |  |  |  |  |
| Policy Group Representative - Tertiary |  |  |  |  |
| EOC Manager - Primary |  |  |  |  |
| EOC Manager - Secondary |  |  |  |  |
| EOC Manager - Tertiary |  |  |  |  |
| Public Information - Primary |  |  |  |  |
| Public Information - Secondary |  |  |  |  |
| Public Information - Tertiary |  |  |  |  |
| External Liaison – Primary |  |  |  |  |
| External Liaison – Secondary |  |  |  |  |
| External Liaison - Tertiary |  |  |  |  |
| Admin Support - Primary |  |  |  |  |
| Admin Support – Secondary |  |  |  |  |
| Admin Support - Tertiary |  |  |  |  |
| Threat Response – Primary |  |  |  |  |
| Threat Response – Secondary |  |  |  |  |
| Threat Response - Tertiary |  |  |  |  |
| Operational Response – Primary |  |  |  |  |
| Operational Response – Secondary |  |  |  |  |
| Operation Response - Tertiary |  |  |  |  |
| Planning and Logistics – Primary |  |  |  |  |
| Planning and Logistics – Secondary |  |  |  |  |
| Planning and Logistics - Tertiary |  |  |  |  |
| Finance – Primary |  |  |  |  |
| Finance – Secondary |  |  |  |  |
| Finance - Tertiary |  |  |  |  |
| Legal – Primary |  |  |  |  |
| Legal – Secondary |  |  |  |  |
| Legal - Tertiary |  |  |  |  |
| IT Resources – Primary |  |  |  |  |
| IT Resources – Secondary |  |  |  |  |
| IT Resources - Tertiary |  |  |  |  |
| Cyber Resources – Primary |  |  |  |  |
| Cyber Resources – Secondary |  |  |  |  |
| Cyber Resources - Tertiary |  |  |  |  |
| Law Enforcement – Primary |  |  |  |  |
| Law Enforcement – Secondary |  |  |  |  |
| Law Enforcement - Tertiary |  |  |  |  |
| <<Indiana City>> Departments – Primary |  |  |  |  |
| <<Indiana City>> Departments – Secondary |  |  |  |  |
| <<Indiana City>> Departments - Tertiary |  |  |  |  |
| Situational Awareness – Primary |  |  |  |  |
| Situational Awareness – Secondary |  |  |  |  |
| Situational Awareness – Tertiary |  |  |  |  |
| Human Resources – Primary |  |  |  |  |
| Human Resources – Secondary |  |  |  |  |
| Human Resources - Tertiary |  |  |  |  |

# Internal Notification Parties

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Internal Parties** | | | | |
| **Department** | **Contact Name** | **Office Phone** | **Cell Phone** | **email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# External Notification Parties

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **External Parties – Vendors, Consultants** | | | | |
| **External Party** | **Contact Name** | **Office Phone** | **Cell Phone** | **email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Operational Planning Process

It was recognized early in the development of the ICS that the critical factor of adequate planning for incident operations was often overlooked or not given enough emphasis. This resulted in poor use of resources, inappropriate strategies and tactics, safety problems, higher incident costs, and lower effectiveness.

Those involved in the original ICS development felt that there was a need to develop a simple but thorough process for planning that could be utilized for both smaller, short-term incidents and events, and for longer, more complex incident planning. The planning process may begin with the scheduling of a planned event, the identification of a credible threat, or the initial response to an actual or impending event. The process continues with the implementation of the formalized steps and staffing required to develop a written Incident Action Plan (IAP).

The primary phases of the planning process are essentially the same for the Incident Commander who develops the initial plan, for the Incident Commander and Operations Section Chief revising the initial plan for extended operations, and for the incident management team developing a formal IAP, each following a similar process. During the initial stages of incident management, planners must develop a simple plan that can be communicated through concise verbal briefings. Frequently, this plan must be developed very quickly and with incomplete situation information. As the incident management effort evolves over time, additional lead time, staff, information systems, and technologies enable more detailed planning and cataloging of events and “lessons learned.”

Planning involves:

* Evaluating the situation.
* Developing incident objectives.
* Selecting a strategy.
* Deciding which resources should be used to achieve the objectives in the safest, most efficient and cost-effective manner.



Caption: Organizational chart showing that Command develops the overall incident objectives and strategy, approves resource orders and demobilization, and approves the IAP by signature. Operations assists with developing strategy, and identifies, assigns, and supervises the resources needed to accomplish the incident objectives. Planning provides status reports, manages the planning process, and produces the IAP. Logistics orders resources and develops the Transportation, Communications, and Medical Plans. Finance/Administration develops cost analyses, ensures that the IAP is within the financial limits established by the Incident Commander, develops contracts, and pays for the resources.

**The Planning “P”**

Diagram

Description automatically generated

|  |
| --- |
|  |

* The Planning “P” is a guide to the process and steps involved in planning for an incident. The leg of the “P” describes the initial response period: Once the incident/event begins, the steps are Notifications, Initial Response & Assessment, Incident Briefing Using ICS 201, and Initial Incident Command (IC)/Unified Command (UC) Meeting.
* At the top of the leg of the “P” is the beginning of the first operational planning period cycle. In this circular sequence, the steps are IC/UC Develop/Update Objectives Meeting, Command and General Staff Meeting, Preparing for the Tactics Meeting, Tactics Meeting, Preparing for the Planning Meeting, Planning Meeting, IAP Prep & Approval, and Operations Briefing.
* At this point a new operational period begins. The next step is Execute Plan & Assess Progress, after which the cycle begins again.

|  |  |
| --- | --- |
| **Initial Response**  Planning begins with a thorough size-up that provides information needed to make initial management decisions.  The ICS Form 201 provides Command Staff with information about the incident situation and the resources allocated to the incident. This form serves as a permanent record of the initial response to the incident and can be used for transfer of command. |  |

|  |  |
| --- | --- |
| **The Start of Each Planning Cycle**   * **IC/UC Objectives Meeting:** The Incident Command/Unified Command establish incident objectives that cover the entire course of the incident. For complex incidents, it may take more than one operational period to accomplish the incident objectives.   The cyclical planning process is designed to take the overall incident objectives and break them down into tactical assignments for each operational period. It is important that this initial overall approach to establishing incident objectives establish the course of the incident, rather than having incident objectives only address a single operational period.   * **Command and General Staff Meeting:** The Incident Command/Unified Command may meet with the Command and General Staff to gather input or to provide immediate direction that cannot wait until the planning process is completed. This meeting occurs as needed and should be as brief as possible. |  |

|  |  |
| --- | --- |
| **Preparing for and Conducting the Tactics Meeting**  The purpose of the Tactics Meeting is to review the tactics developed by the Operations Section Chief. This includes the following:   * Determine how the selected strategy will be accomplished in order to achieve the incident objectives. * Assign resources to implement the tactics. * Identify methods for monitoring tactics and resources to determine if adjustments are required (e.g., different tactics, different resources, or new strategy).   The Operations Section Chief, Safety Officer, Logistics Section Chief, and Resources Unit Leader attend the Tactics Meeting. The Operations Section Chief leads the Tactics Meeting.  The ICS Forms 215, Operational Planning Worksheet, and 215A, Incident Safety Analysis, are used to document the Tactics Meeting.  Resource assignments will be made for each of the specific work tasks. Resource assignments will consist of the kind, type, and numbers of resources available and needed to achieve the tactical operations desired for the operational period. If the required tactical resources will not be available, then an adjustment should be made to the tactical assignments being planned for the Operational Period. It is very important that tactical resource availability and other needed support be determined prior to spending a great deal of time working on strategies and tactical operations that realistically cannot be achieved. | Graphical user interface, application, Word  Description automatically generated |

|  |  |
| --- | --- |
| **Preparing for the Planning Meeting**  Following the Tactics Meeting, preparations are made for the Planning Meeting, to include the following actions coordinated by the Planning Section:   * Review the ICS Form 215 developed in the Tactics Meeting. * Review the ICS Form 215A, Incident Safety Analysis (prepared by the Safety Officer), based on the information in the ICS Form 215. * Assess current operations effectiveness and resource efficiency. * Gather information to support incident management decisions. |  |

|  |  |
| --- | --- |
| **Planning Meeting**  The Planning Meeting provides the opportunity for the Command and General Staff to review and validate the operational plan as proposed by the Operations Section Chief. Attendance is required for all Command and General Staff. Additional incident personnel may attend at the request of the Planning Section Chief or the Incident Commander. The Planning Section Chief conducts the Planning Meeting following a fixed agenda.  The Operations Section Chief delineates the amount and type of resources he or she will need to accomplish the plan. The Planning Section’s “Resources Unit” will have to work with the Logistics Section to accommodate.  At the conclusion of the meeting, the Planning Section Staff will indicate when all elements of the plan and support documents are required to be submitted so the plan can be collated, duplicated, and made ready for the Operational Period Briefing. |  |

|  |  |
| --- | --- |
| **IAP Preparation and Approval**  The next step in the Incident Action Planning Process is plan preparation and approval. The written plan is comprised of a series of standard forms and supporting documents that convey the Incident Commander’s intent and the Operations Section direction for the accomplishment of the plan for that Operational Period.  For simple incidents of short duration, the Incident Action Plan (IAP) will be developed by the Incident Commander and communicated to subordinates in a verbal briefing. The planning associated with this level of complexity does not demand the formal planning meeting process as highlighted above.  Certain conditions result in the need for the Incident Commander to engage a more formal process. A written IAP should be considered whenever:   * Two or more jurisdictions are involved in the response. * The incident continues into the next Operational Period. * A number of ICS organizational elements are activated (typically when General Staff Sections are staffed). * It is required by agency policy. * A Hazmat incident is involved (required). |  |

|  |  |
| --- | --- |
| **Operations Period Briefing**  The Operations Period Briefing may be referred to as the Operational Briefing or the Shift Briefing. This briefing is conducted at the beginning of each Operational Period and presents the Incident Action Plan to supervisors of tactical resources.  Following the Operations Period Briefing supervisors will meet with their assigned resources for a detailed briefing on their respective assignments. |  |

|  |  |
| --- | --- |
| **Execute Plan and Assess Progress**  The Operations Section directs the implementation of the plan. The supervisory personnel within the Operations Section are responsible for implementation of the plan for the specific Operational Period.  The plan is evaluated at various stages in its development and implementation. The Operations Section Chief may make the appropriate adjustments during the Operational Period to ensure that the objectives are met and effectiveness is assured. |  |

# Incident Action Plan Forms

## Incident Action Plan (IAP) Quick Start

(available electronically at: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

|  |  |
| --- | --- |
| **1. Incident Name** | **2. Operational Period** (# )  Date: From: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ To: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Time: From: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ To: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **3. Situation Summary** | |
| **4. Current Incident Management Team** (f ill in additional positions as appropriate) | |

|  |  |  |  |
| --- | --- | --- | --- |
| **5. Health and Safety Briefing** Identify any potential incident health and safety hazards and develop necessary measures (remove hazard, provide personal protective equipment, warn people of the hazard) to protect responders from those hazards. | | | |
| **6. Incident Objectives** | | | |
| **6a. OBJECTIVES** | **6b. STRATEGIES / TACTICS** | **6c. RESOURCES REQUIRED** | **6d. ASSIGNED TO** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **7. Prepared by:**  PRINT NAME: \_ SIGNATURE:  DATE/TIME: \_ FACILITY: | | | |

## Activity Log

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activity LOG** | | 1. Incident Name | 2. Date Prepared | | 3. Time Prepared |
| 4. Functional Group | | 5. Group Leader (Name and Position) | | | 6. Operational Period |
| 7. Personnel Roster Assigned | | | | | |
| Name | | Role | | Location/Contact Info | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
| 8. Activities | | | | | |
| Time | Major Events | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
|  |  | | | | |
| 9. Prepared by (Name and Position) | | | | | |

## ICS 213 General Message Form

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **GENERAL MESSAGE** | | | | | |
| **TO**: | | | POSITION: | | |
| FROM: | | | POSITION: | | |
| SUBJECT: | | | DATE: | | TIME: |
| MESSAGE: | | | | | |
|  | | | | | |
| SIGNATURE: | | | | POSITION: | |
| REPLY: | | | | | |
|  | | | | | |
| DATE: | TIME: | SIGNATURE/POSITION: | | | |