# Project Security Incident Response Procedures

## Contents

* [Introduction](#introduction)
* [Roles and Responsibilities](#roles-and-responsibilities)
  + [Responder](#responder)
  + [Incident Commander](#incident-commander)
  + [Communications Officer](#communications-officer)
* [Incident response process](#incident-response-process)
  + [1. *Breathe*](#Xb4b48fa8c0f847b8816c4c860b3512d23c7e67b)
  + [2. Start documenting](#X3b1b20e2347843f39d5953a39da29e37d8adbb2)
  + [3. Initiate the response](#X3f2d323b76ed36513876ff9d909858b1ae46a72)
  + [4. Assess the incident](#X230ed7165574a31fdc03331b44d05d7dc2a7c28)
  + [5. Remediate](#Xfdd7bfe7795a0ffefd856a48770679880652805)
  + [6. Conclude the incident](#X58331d5904117288742acdba7d04aa489b8f6ac)
* [Incident severities](#incident-severities)
  + [High severity](#high-severity)
  + [Medium severity](#medium-severity)
  + [Low severity](#low-severity)
* [Explicit Handoff Ceremony](#explicit-handoff-ceremony)

## Introduction

This document describes the Project Full Name Incident Response Team’s process for responding to security incidents and other disruptions that may affect the Confidentiality, Integrity, Availability (CIA) or Privacy of system resources and data. It explains:

* roles and responsibilities during and after incidents
* overview of the steps to follow for resolution

*During an incident, the* [*IRP checklist*](security-irp-checklist.md) *may be more useful as it contains bulleted, actionable items for the IR Team to follow.*

## Roles and Responsibilities

Individual and team roles are described below.

### Responder

A *Responder* is a member of the Project Full Name IR Team that investigates and remediates an event or incident.

#### First Responder

The *First Responder* is the first IR Team member who becomes aware of the incident.

* Frequently the *First Responder* is also the incident *Reporter*.
* The *First Responder* assumes the role as the initial *Incident Commander (IC)* until IC duties are [handed off](#explicit-handoff-ceremony).
* For the first 15-30 minutes, the *First Responder* may be the only responder. If needed, the *First Responder* begins forming the IR Team. See [Initiate](#X50b2c6d3dd2a1397fcb697b3112b1a38cd4406c).

#### IR Team Responders

During incident response, *Responders* do the following:

* Assume primary responsibility for the [Assess](#X0a2568bf01c95746c92753b3e5e60ac10ccc387) and [Remediate](#Xe294158153b9337b5ad3543226588fe5929df6b) steps.
* Document in real time the measurements, theories, and steps taken using the Slack channel [#None](None) or other channels provided by the IC.
* Designate an *Incident Commander*, if the incident might require more than 15-30 minutes to resolve, and do an [explicit hand-off](#explicit-handoff-ceremony).

### Incident Commander

The *Incident Commander (IC)* remains uninvolved in remediation efforst, and performs three major duties:

1. IR Team creation and management, ensuring that the IR Team:
   * Includes team members who are capable of containing, investigating, and remediating the incident.
   * Remains focused on resolving the incident.
   * Uses the most appropriate media/communication channels for recording actions. During business hours, a dedicated Slack channel (for example, `#fire-team) may be created for IR Team communications.
   * Utilizes work shifts if the incident lasts longer than 3 hours.
2. Documentation, which includes all actions taken during investigation and remediation:
   * Initially in the Slack channel [#None](None).
   * Also in the Project JIRA ticket.
3. Communication, which ensures that internal and external entities are apprised of the situation and includes progress reports. For communication duties, the IC may designate a *Communications Officer* (CO) and do an [explicit handoff](#explicit-handoff-ceremony).

### Communications Officer

Communication is critical as the IR Team works to contain, investigate, and remediate an incident.

The Incident Commander (IC) manages communications regarding the incident until [handing off IC duties](#explicit-handoff-ceremony) to another IR Team member or unless a Communications Officer (CO) is designated.

The CO manages external communications with:

* Management, developers, users, and anyone affected by the incident
* Client stakeholders
* Additional Project team members and/or the Product Owner when needed
* Legal team and US-CERT, if escalation is required

#### Communication channels

* Slack channel [#None](None). (Using @channel sends a Slack notification to everyone in the channel.)
* During business hours, a dedicated Slack channel (for example, #fire-team) may be created for IR Team communications.
* A Project [JIRA Incident ticket](https://project.atlassian.net/issues/?jql=issuetype=Incident) is be the final location for all incident reporting, with links to other documents as needed.
* Zoom, Meet, or other video conference. (Not recommended for recording actions as the record can be lost when the call ends.)
* Email to TheProject@example.com. (This alerts all on-call responders.)
* [CivicActions/Project IR Team contacts](None). (Provides direct email addresses and phone numbers.)

## Incident response process

There are six major processes of incident response, detailed below:

* [1. *Breathe*](#Xc796357300b0134deb140e661652db8c9559503)
* [2. Start documenting](#X13134437a84608ccc16204cf17d9f062d09a0d5)
* [3. Initiate the response](#X50b2c6d3dd2a1397fcb697b3112b1a38cd4406c)
* [4. Assess the incident](#X0a2568bf01c95746c92753b3e5e60ac10ccc387)
* [5. Remediate](#Xe294158153b9337b5ad3543226588fe5929df6b)
* [6. Conclude the incident](#Xc60e765e8354a7d5794abd5764f6484daa1ca4c)

*During an incident, the* [*IRP checklist*](security-irp-checklist.md) *may be more useful as it contains bulleted, actionable items for the IR Team to follow.*

### 1. *Breathe*

No one’s life is in danger.

### 2. Start documenting

Begin documenting all steps and findings. Documentation makes handoffs and responder onboarding easier. The Slack channel [#None](None) is recommended because it is most widely accessible, but other [communication channels](#communication-channels) may be used.

### 3. Initiate the response

At this stage, the *First Responder* is usually working alone, and is also the *Incident Commander* (IC).

A. Allocate 5 minutes and determine whether this event is a potential incident or false alarm.

An incident begins when someone becomes aware of a disruption in expected normal system operations. The definition of “incident” is broad, following [*NIST SP 800-61: Computer Security Incident Handling Guide*](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final), as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices”. This definition encompasses any scenario that might threaten the security of the Project Full Name. For more information, see the CivicActions handbook: [What is an incident?](http://civicactions-handbook.readthedocs.io/en/latest/09-security/incidents/#what-is-an-incident)

When noticing what appears to be a Project-related event, the Project team member should check normal communication channels, such as the Slack channel ([#None](None)), to determine whether this could be expected behavior (for example, system downtime during a maintenance window). If it appears to be a valid incident, the Project team member becomes the *Reporter* and alerts the on-call responders via the Slack channel ([#None](None)) or email TheProject@example.com. If no one from the IR Team acknowledges the message within 10 minutes, the *Reporter* should escalate the issue by contacting Project team members on the <None> contact sheet directly until someone acknowledges the report.

B. Respond accordingly:

* **Potential incident**
  1. Issue a broadcast notification via one or more of the following:
     + Slack channel [#None](None). Use @channel to notify the Project team. This may have been automatic via OpsGenie pager alarms.
     + Email to the on-call system admin: TheProject@example.com
     + Email/telephone to <None>
  + An example message follows. The format is not important, but the information fields are useful.
  + \*\*Description\*\*: \_[Short description of the event and its impact]\_  
     \*\*Status\*\*: investigating  
     \*\*Severity\*\*: unknown  
     \*\*Reporter\*\*: \_[name of the person who reported the issue]\_  
     \*\*IC\*\*: \_[your name]\_  
     \*\*Responders\*\*: \_[names of other responders]\_  
     \*\*Details\*\*: \_[Any extra details about the event can go here.]\_
  + Observe the following guidelines for communications:
  + - During this stage of incident response, the event status is "investigating".   
     - An unconfirmed issue is called an \_event\_. A confirmed issue is called an \_incident\_.
  1. For an incident requiring more than 30 minutes to resolve:
     + Recruit additional IR Team responders via the Slack channel [#None](None).
     + Designate an [Incident Commander](#incident-commander) and [hand off the IC duties](#explicit-handoff-ceremony).
     + More information on [incident response roles and responsibilities](#roles-and-responsibilities):
       - [Responder](#responder)
       - [Incident Commander (IC)](#incident-commander)
       - [Communications Officer (CO)](#communications-officer)
     + Use the [*Explicit Handoff Ceremony*](#explicit-handoff-ceremony) when transferring/changing roles.
* **False alarm**
* Conclude the incident. Proceed to [*6. Conclude the incident*](#X144ffe43bf2dce94ae1eaca47aadcb511f671f8).

### 4. Assess the incident

#### IR Team responsibilities during assessment

A. Confirm the incident.

1. Gather information, and document your findings.  
  
 - Was the event triggered by an [external dependency](contingency-plan.md#external-dependencies)?  
 - Is a system failure causing the disruption?  
  
 2. Proceed to the next step for a confirmed incident. (For a false alarm, conclude the incident. Proceed to [\_6. Conclude the incident\_](#6.-conclude-the-incident).)

B. Assess the severity.

- Use the [rubric for determining severity](#incident-severities). (Project incidents are generally "Low severity".)  
 - Does it affect system or data Confidentiality, Integrity, Availability and/or Privacy?  
 - Note that severity can change over the lifespan of an incident, and it is acceptable for the IR Team to assess the initial severity quickly.

C. Determine whether the IR Team needs to activate the [Contingency Plan](contingency-plan.md). Consider whether Disaster Recovery is required.

The IR Team should record all actions and observations in an appropriate [communication channel](#communication-channels).

*Reminder: Use the* [*Explicit Handoff Ceremony*](#explicit-handoff-ceremony) *when transferring/changing roles.*

#### Incident Commander responsibilities during assessment

* Post an initial situation report (*sitrep*), in the following locations:
  + JIRA ticket
  + Slack channel [#None](None) (include link to [JIRA Incident ticket](https://project.atlassian.net/issues/?jql=issuetype=Incident))
  + Any other [communication channels](#communication-channels) as indicated by the IC (or CO).
* Here is an example sitrep:
* \*\*Subject\*\*: [sitrep] The chickens are escaping  
  \*\*Severity\*\*: low  
  \*\*IC\*\*: Farmer Jane  
  \*\*Responders\*\*: Spot the Dog, Farmer Dave  
  \*\*Description\*\*: We've confirmed reports of escaped chickens. Looks like a fox may have tunneled into the run. Dave is working to fix the fence. Spot is tracking the fox.
* Ensure that a JIRA ticket has been created. This should be done, even if the *First Responder/IC* manages the incident fully, for example, by simply restarting a service.

### 5. Remediate

Remediation is about resolving the issues caused by an incident. Remediation will be situation-specific, and timelines vary based on the assessed severity.

#### Remediation and service disruption

Remediation may require service disruption. If it does, the IR Team should proceed in a different way depending on the [severity](#incident-severities):

* **High severity**: Take action immediately, even if this causes disruption. A notification about the disruption should be sent out as soon as possible, but the IR Team needs no permission to take action at this level.
* **Medium severity**: Notify the Project leads about the planned action, and help them assess the relative risk of disruption versus security. If the leads are unavailable on Slack, contact them using the phone numbers in their Slack profiles. The Project team should reach a collaborative decision on action, with a bias towards disruption. If they cannot be reached within an hour, the IR Team may take action without them.
* **Low severity**: Notify the Projectleads as described above. Do not take action until a mutually-agreed course of action has been determined.

#### Remediation requiring more than 3 hours

Remediation takes time. If the issue progresses for more than 3 hours without being resolved, the IC should plan for a long remediation. This means:

* The IC determines whether remediation efforts will occur during business hours only or be continuous. This depends on the severity of the issue, and whether breaches are ongoing.
* For a continuous response, the IC should plan shifts. This allows responders to take breaks and insures continuous coverage. Shifts should be no longer than 3 hours. Also, the IC duties should rotate in shifts no longer than 3 hours.

#### IR Team responsibilities during remediation

* Determine the cause, implement a resolution, and return the system to normal operations. Make every attempt to identify the cause; this can prevent incident recurrence.
* Maintain a list of informational leads from the incident — actionable information about any security breaches, stolen data, etc.
* Develop a list of remediation steps. These can be tracked as checklists in the [JIRA Incident ticket](https://project.atlassian.net/issues/?jql=issuetype=Incident).

If suspicious activity is suspected or other unanswered questions exist, do the following before making any changes:

* Make backup snapshots of relevant volumes and data.
* Preserve logs.
* Take screen captures of anomalous activity that can be used in post-remediation forensic analysis.
* Consider implementing a containment strategy. For example, reconfigure firewall rules for the affected instance to drop all ingress and egress traffic, except from specific IPs like your own, until forensics can be performed.

#### Incident Commander responsibilities during remediation

At a high level, the IC tracks remediation actions, ensures they are assigned and followed, and verifies them when they are completed. (Remediation efforts may be tracked with the issue details.)

The IC must distinguish between immediate concerns, which need to be completed before the incident is considered resolved, and long-term improvements/hardening, which can be deferred to the Retrospective.

The IC does do the following:

* Maintains current information in Slack, shared Google Docs files, the [JIRA Incident ticket](https://project.atlassian.net/issues/?jql=issuetype=Incident), or other [communication channels](#communication-channels). Be sure to include:
  + Project team leads and members
  + Remediation items and their assignees
* Establishes and documents work shifts for an incident longer than 3 hours.
* Maintains communications with stakeholders, or designates a *Communications Officer* via [explicit handoff](#explicit-handoff-ceremony).
* Shares sitreps on a regular basis:
  + High severity: hourly
  + Medium severity: 2x daily
  + Low severity: daily
* Focuses on coordination, communication, and information collection – not remediation.

#### Communications during remediation

The *Incident Commander* (IC) or *Communications Officer* (CO) does this following:

* Coordinates with the CivicActions managers to apprise them of the situation.
* Coordinates with the Project Full Name Product Owner (PO) to notify affected customers.
* Ensures that the IR Team is recording all actions in the appropriate designated [communication channels](#communication-channels).
* Shares sitreps on a regular basis in Slack, in the [JIRA Incident ticket](https://project.atlassian.net/issues/?jql=issuetype=Incident), and with stakeholders. See the section on [incident severities](#incident-severities) for suggested time intervals for each severity level.

### 6. Conclude the incident

#### Closing the JIRA ticket

When the incident is no longer active, for example, the breach has been contained, the issue has been fixed, etc., the IC should conclude the incident. There might be longer term remediation required, and possibly more investigation, but when the incident is no longer active, these activities can proceed at the regular pace of business.

To conclude an incident, the IC should:

* Set the status of the incident to **Ready for QA**.
* Send a final sitrep to stakeholders.
* Thank everyone involved for their service.

#### Conducting a retrospective

The IC (one IC if there were multiple ICs, or another designated party such as the Communications Officer) should lead a retrospective and develop an incident report.

#### Developing the incident report

The incident report should contain:

* a timeline of the incident
* details about how the incident progressed
* information about the vulnerabilities that led to the incident, also called a *cause analysis* (The *cause analysis* is an important part of the incident report. Tools such as [Infinite Hows](https://www.kitchensoap.com/2014/11/14/the-infinite-hows-or-the-dangers-of-the-five-whys/) and [Five Whys](https://en.wikipedia.org/wiki/5_Whys) can help the IR Team explore potential causes, prevention, and improved incident response.)

Additionally, the incident report should include basic response metrics:

* **Discovery method**: How did the IR Team become aware of the issue?
* **Time to discovery**: How much time passed from the time the incident became active until someone became aware of it?
* **Time to containment**: How much time passed from the time someone became aware of the incident until the incident was contained?
* **Threat actions**: What actions were taken by the actor? For example, phishing, password attacks, etc.

The incident report should be posted as a final comment on the JIRA ticket, and then the JIRA ticket should be closed.

## Incident severities

The incident severity level determines the actions of the IR Team. Severity usually changes during the lifecycle of the incident.

### High severity

A high severity incident does one or more of the following:

* compromises the confidentiality/integrity of Sensitive Personally Identifiable Information (SPII),
* impacts the availability of services for a large number of customers, or
* has significant financial impact.

Examples include:

* Confirmed breach of SPII
* Successful root-level compromise of production systems
* Denial of Service attacks resulting in severe outages

Guidelines for incident response:

* Remediation efforts will likely be continuous until the issue is contained.
* Responders may take any action required to contain the issue, including complete service degradation.
* Sitreps should be shared every hour, or more frequently.

### Medium severity

A medium severity incident can be an unsuccessful attempt to breach Personally Identifiable Information (PII), an event with limited impact on the availability of services for a large number of customers, or an event with limited financial impact. Examples include:

* Suspected PII breach
* Targeted but unsuccessful attempts to compromise production systems
* Spam/phishing attacks targeting CivicActions or Project staff
* Denial of Service attacks resulting in limited service degradation

Guidelines for incident response:

* Response should occur during business hours.
* Responders should attempt to consult stakeholders before causing downtime, but may proceed without consent if stakeholders do not respond in a reasonable time frame.
* Sitreps should be shared approximately twice per day.

### Low severity

A low severity incident does not affect PII, and has no availability or financial impact. Examples include:

* Attempted compromise of non-important systems, for example, staging or testing instances
* Denial of Service attacks with no noticeable customer impact

Guidelines for incident response:

* Response should occur during business hours.
* Responders should avoid service degradation unless stakeholders agree.
* Sitreps should be shared daily.

## Explicit Handoff Ceremony

To transfer *Incident Commander*, *Communications Officer* or *Responder* (“ROLE”) duties:

1. Outgoing ROLE initiates the handoff and briefs the incoming ROLE on the situation.
2. Incoming ROLE confirms the handoff and assumes responsibility.
3. Incoming ROLE updates the JIRA ticket and notes the handoff.
4. Incoming ROLE shares a *sitrep*, which notes the handoff.
5. Outgoing ROLE remains available for 15-20 minutes to ensure a smooth handoff and then logs off.