# Project Security Incident Response Procedure Checklist

This checklist provides incident response procedures. For more detail, see the [Security Incident Response Plan](security-irp.md).

## Contents

* [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)

## 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](security-irp.md#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.

B. Respond accordingly:

* **Potential incident**
  1. Issue a [broadcast notification](security-irp.md#communications-during-the-initiate-phase) 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 “on call” system admin: TheProject@example.com
     + Email/telephone to [CivicActions/Project IR Team](None)
  2. 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**](security-irp.md#incident-commander) and [hand off the IC duties](security-irp.md#explicit-handoff-ceremony).
     + More information on [incident response roles and responsibilities](security-irp.md#roles-and-responsibilities):
       - [Responder](security-irp.md#responder)
       - [Incident Commander (IC)](security-irp.md#incident-commander)
       - [Communications Officer (CO)](security-irp.md#communications-officer)
     + Use the [*Explicit Handoff Ceremony*](security-irp.md#explicit-handoff-ceremony) when transferring/changing roles.
* **False alarm**
* Conclude the incident. Proceed to [*6. Conclude the incident*](#conclude-the-incident).

## 4. Assess the incident

**IR Team responsibilities**

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*](#conclude-the-incident).)

B. Assess the severity. Use the [rubric in the IR guide](security-irp.md#incident-severities). (Project incidents are generally “Low severity”.)

C. Assess whether to activate the [contingency plan](contingency-plan.md). Consider whether Disaster Recovery is required.

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

**Incident Commander responsibilities**

* Post an initial situation report, called a *sitrep* ([example sitrep](security-irp.md#assess)), to the Slack channel [#None](None). Include a descriptive name, and identify the current Incident Commander and Responders.
* 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 re-starting a service.

## 5. Remediate

**IR Team responsibilities**

* 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.
* 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 yours, until forensics can be performed.

**Incident Commander responsibilities**

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

## 6. Conclude the incident

A. Update the JIRA ticket and set the status to one of the following:

* Confirmed incident: *Ready for QA*
* False alarm: *Done*

B. Notify the Slack channel [#None](None) that the incident has been resolved.

C. Schedule an [IR Team retrospective](security-irp.md#have-a-team-retrospective). Optional for false alarms.

D. Share the final *sitrep* with stakeholders.

E. Thank everyone for their service.