Incident Checklist

> The Incident Checklist provides a standardized form for administrators and investigators to ensure all critical investigative steps are completed before closing an incident. Its primary purpose is to help maintain comprehensive, consistent, and legally sound records for audits and internal reviews. This article is intended for OperationsCommander (OPSCOM) administrators and security personnel responsible for managing and closing incident reports.

Setup and Configuration

The Incident Checklist is a core component of the IncidentAdmin module and requires no additional system setup. However, administrators must have the appropriate permissions to view and edit incidents to access and complete this form.

Using this Feature

Administrators must navigate to an active incident report to access and fill out the checklist. The form requires users to select standard responses (e.g., Yes, No, Not Required) and provide clarifying remarks for each step of the investigation.

Accessing the Checklist

1. Navigate to and open the specific incident you wish to update.
2. Click the **Checklist** tab within the incident record.

3. Click the **Open Checklist** button to launch the form.

> Depending on your organization's specific subcategory configurations, filling out this checklist may be a mandatory system requirement before an administrator is permitted to close the incident report.

Checklist Fields Defined

When filling out the checklist, provide specific details in the remarks fields to justify your selections.

- **CCTV Reviewed**: Indicate if closed-circuit cameras were reviewed. State what was found in the footage or explain why the footage was not reviewed.
- **Other Resources Reviewed**: Indicate if external resources were utilized, such as social media, public directories, or OPSCOM records.
- **Witness(es) Interviewed**: Note if witnesses were spoken to and summarize their specific contributions to the incident resolution.
- **Suspect(s) / Person(s) of Interest Interviewed**: Document any suspect interviews, noting their involvement or statements.
- **Statements Obtained**: Confirm if formal, written statements were collected from any involved parties.
- **Other Evidence Collected**: Detail any physical or virtual evidence gathered (e.g., photos, physical items) and note its secure storage location.
- **Safe Plan and Community Resources Discussed with Complainant**: Note if the complainant was provided with a safety plan or referred to external support resources.

- **Other Departments / Agencies Consulted or Notified**: List any internal departments (e.g., Student Housing) or external agencies (e.g., local police) that were briefed on the incident.
- **Community Notified**: State if and how the broader community was alerted to the incident (e.g., safety bulletins, campus emails).
- **Security / CPTED Audit Conducted**: Indicate if a Crime Prevention Through Environmental Design (CPTED) or general security audit was performed. Note any vulnerabilities discovered and the steps taken to resolve them.
- **Recommendations Made to Prevent a Re-occurrence**: Detail any operational or security changes suggested to prevent future similar incidents.
- **Complainant Notified of Outcome**: Confirm that the reporting party was updated on the final resolution of the case.
- **Documentation Updated & Filed**: Note exactly where related files, audits, or hard copies were saved.
- **Status at time of Closing**: Select the final state of the case (Solved, Unsolved, or Unfounded).
- **Reason For Report Being Closed**: Click the drop-down menu and choose the primary reason for closing the report.
- **Closing Comments**: Provide a final narrative summarizing the resolution and confirming any implemented recommendations.

Best Practices and Considerations

- **Standardize Remarks: Organizations should develop a business rule outlining the minimum level of detail required in the remarks section.** Simple "Yes" or "No" answers without context can

lead to poorly documented investigations.

- **Complete Before Closing:** Ensure all relevant checklist fields are thoroughly completed before attempting to change the overall incident status to closed.

Revision #4
Created 14 May 2024 07:13:47
Updated 12 August 2026 12:30:14