Ethics and Standards Review

Internal Investigation Framework

Standard Committee

Purpose
This framework establishes a standardized approach for conducting internal investigations to ensure a fair, consistent, and thorough process. It safeguards the integrity of organizational procedures, accountability, and confidentiality.

---

0. Confidentiality

- **Confidentiality Guidelines:**
  Confidentiality is critical for protecting all involved parties and ensuring the investigation’s integrity. Information regarding the investigation should only be accessible to the designated review team. No information may be shared outside the review team unless expressly authorized. If confidentiality is compromised, the audit team may remove the affected member's testimony or declare the review invalid.
- **Data Handling Protocols:**
  All documentation and records should be securely stored with restricted access to authorized personnel only.

1. Initiation of Investigation

- **Trigger for Investigation:**
  Investigations may be initiated in response to:
  - Reported incidents (e.g., policy violations, misconduct, safety concerns).
  - Identified risks or potential process failures.
  - Management observations or flagged audit results.
- **Authorization Requirements:**
  Investigations require authorization from two or more board members who are not implicated in the incident to maintain objectivity.
- If all board members are implicated, a vote may appoint an internal audit lead or approve a third-party audit for impartiality.

2. Scope and Objectives

- **Define Scope:**
  Clearly define the scope of the investigation, including specific allegations, individuals, processes, or policy areas to be addressed. Ensure alignment with organizational policies and standards.

- **Set Objectives:**
  Identify what the investigation aims to achieve, such as:
  - Uncovering relevant facts and establishing timelines.
  - Determining the root cause of the incident or behavior.
  - Identifying gaps in policies or procedures.
- **Timeline:**
  Set a realistic timeline for completing the investigation and communicate this to relevant stakeholders.
- **Scope Document:**
  Develop a formal scope document detailing the objectives and limits of the investigation.
- - This document, prepared by the investigation team, must be finalized before the investigation begins.
    - If the investigation scope changes, an amendment to the document should be submitted.
    - The scope document should contain only essential information and be prepared for press-level scrutiny, without confidential data.

3. Investigative Team Selection

- Team Composition:
  Choose team members based on relevant expertise, impartiality, and authority. Representatives from essential departments may be included.
- Conflict of Interest Check:
  All team members must declare any conflicts of interest to ensure objectivity.
- Roles and Responsibilities:
  Assign specific roles, such as lead investigator, interviewer, and evidence manager, to maintain clarity and avoid duplication.
- - Team members may assume multiple roles, depending on team size and investigation complexity.

4. Planning the Investigation

- Background Research:
  Gather initial information relevant to the incident, such as prior incidents, records, or applicable policies.
- Investigation Plan:
  Develop a detailed plan that includes:
- - Key activities like document reviews and interviews.
    - Sources of information and data to be examined.
- Legal and Compliance Considerations:
  Ensure all steps comply with local laws, labor regulations, and internal policies. Organizational policies do not supersede anylocal legal requirements.

5. Evidence Collection

- **Document and Data Review:**
  Collect all pertinent records, including emails, reports, logs, and any process documentation.
- **Interviews and Statements:**
  Interview involved individuals and relevant witnesses.
- ○ Use open-ended, unbiased questions and document all responses.
- **Preservation of Evidence:**
  Securely back up physical and digital evidence to prevent tampering or data loss.
- ○ Cloud backups should be maintained securely.
  - ○ Any loss of information may lead to a formal warning or removal from the review team, depending on the severity.

6. Analysis and Evaluation

- Review and Analyze Evidence:
  Carefully evaluate all evidence to confirm facts, timelines, and compliance with relevant policies.
- Identify Gaps and Causes:
  Pinpoint procedural or operational gaps that may have contributed to the issue.
- Accountability and Impact Assessment:
  Based on findings, assess the accountability of individuals and the organizational impact of the incident.

7. Documentation and Reporting

- **Prepare a Detailed Report:**
  Summarize findings, analyses, and recommendations, including:
- ○ Investigation overview.
  - ○ Key evidence and factual conclusions.
  - ○ Accountability determinations, if applicable.
- **Recommendations:**
  Provide actionable recommendations, which may include:
- ○ Disciplinary actions.
  - ○ Policy or procedural improvements.
  - ○ Staff training or awareness initiatives.
- **Review and Approval:**
  Submit the report to the board for review, approval, and further action.

8. Communication of Findings

- **Internal Communication:**
  Share findings with relevant parties while respecting confidentiality.
- ○ Major findings should be communicated via email with all team members cc’d.
  - ○ Communication between team members should occur within a designated group chat involving the majority of the team.

    - Unauthorized communication outside the group chat is subject to disciplinary action.
- **Feedback Loop:**
  Provide each individual interviewed with a transcript of their statements.
- ○ Individuals have 24 hours to request amendments or redact sensitive information before the document is finalized.

9. Post-Investigation Actions and Follow-Up

- **Implement Recommendations:**
  Collaborate with relevant departments to implement any recommended actions and monitor completion.
- **Track Progress and Effectiveness:**
  Regularly review the effectiveness of implemented changes to address any new issues promptly.
- **Policy Review:**
  Update investigation policies and procedures as necessary to reflect insights gained and best practices.

10. Documentation and Record-Keeping

- **Record Retention:**
  Securely retain all investigation documentation per organizational policy and relevant legal requirements.
- **Confidentiality and Access Control:**
  Restrict access to investigation records to authorized personnel only, ensuring compliance with confidentiality protocols.

Revision #4
Created 19 December 2024 03:33:48 by Joanna Fang
Updated 20 December 2024 00:47:48 by Joanna Fang