Creating or Updating Your Whistleblowing Policy

A GUIDE TO DETERMINING THE BEST FIT AND VALUE FOR YOUR ORGANIZATION

CORNERSTONE
GOVERNANCE CORPORATION

Forward

There are several factors to consider when creating or updating the whistleblowing process for your organization. Although at first thought it may seem like simply setting up an internal dedicated telephone / fax hotline, email address or web submission is all that is necessary; but how do you ensure the requirements of anonymity and resolution are met? It is important to analyze the needs of your organization to ensure the policy created fits those needs.

Following are some key questions to consider when creating or updating your whistleblowing policy.

For more information on the services we provide, including our incident reporting system to enhance your whistleblowing policy, please view our website or contact us.

Best Regards,

Suzanne Ferguson

President

Cornerstone Governance Corp.

Should I use an internal or external system?

Internal system considerations

Consider the following issues when determining whether to use an internal system:

Issues	Questions
Personnel	• Will employees trust that an internal system is truly confidential or will they be afraid that their anonymous submissions will be traced back to them? • Who will you entrust to receive reports and with whom will they be shared with? • Does your organization have offices and operations in multiple cities? If so, how will you handle reports made in a different language? Will you have a designated investigator locally or will everything be filtered through head office? • Will there be a process is place to ensure reports are not left unsecured? • Who will cover vacation time or unexpected leave for the designated recipient? • Who will take over if the designate leaves the organization? • Who will train the new designate on the process to receive and investigate reports?
Technical	• Can an email submission truly keep the sender's information anonymous? • Would the IT department be able to access a report received electronically by email or web portal? • Can an IT employee within the organization working to resolve a technical issue have access to confidential information? • Will phone and fax numbers be password protected? Who will have access to them and how often will they be changed? Who will monitor and maintain the necessary infrastructure? • Will your internal system be accessible from outside the office network or only internally via the intranet or internal telephone system?

External or Third Party System benefits

External or third party systems have the following benefits:

- Employees will feel confident using a truly anonymous reporting system and will be more comfortable submitting a report
- No system monitoring or maintenance is required by an organization saving time, money and IT resources.

Continued on next page …

… continued from previous page.

- Training and ongoing support are developed and provided by the third party service provider saving internal resources for other projects
- Additional resource can be sourced when needed e.g., forensic auditor or human resource investigator
- Confidentiality is of the utmost importance – a third party monitoring system may help to define your policy requirements further

What issues should be reported through the incident reporting system?

Policy clearly defines

Your whistleblowing policy should clearly define the issues you want reported. It should also include the different channels available to employees e.g., speaking to a supervisor, human resources and submitting a report through your incident reporting system.

> If an employee holds information that they believe shows that a fraud or harassment issue is occurring, they may not be comfortable bringing this information to their supervisor. They may elect to use an anonymous submission to make their report.
>
> If the issue is that the employee is upset the organization is not hosting a Christmas Party this year, this concern should be brought up with the employee' supervisor or human resource department rather than submission through the incident reporting system.

Common issues to use as examples in your policy

Common issues to use as examples in your policy or during orientation and training with employees may include, but is not limited to:

Issue	Examples
Code of Conduct Violations	• Theft • Fraud • Bullying • Harassment • Discrimination • Insider trading • Accepting kickbacks • Bribery

Continued on next page …

… continued from previous page.

Theft and fraud	• Petty cash theft • Skimming of cash • Phony invoices • Ghost employees • Filing false expense reports • Forging cheques
Other relevant or industry specific	• Environmental hazards • Drug and alcohol use • Privacy or security breaches

How will you communicate your whistleblowing policy?

Communicating your policy

Communication is imperative when implementing a new policy or updating your current one to ensure everyone understands the process. Providing examples of issues that you want your employees and stakeholders e.g., contractors, suppliers or members to be on the lookout for will help them to be more aware of their surroundings and be more comfortable knowing they are doing the right thing by submitting a report.

Consider the following opportunities to get the word out:

Opportunity	Details
Initial Orientation or Department Meeting	• The policy should be covered in an employee's initial orientation or a department or organization-wide meeting may be held for rollout. • A walkthrough of the reporting process and how to use the incident reporting system will help employees feel more engaged with the policy. Providing support materials to take home to give them comfort knowing they can access and review the information privately.
Ongoing reminders	• Ongoing reminders with pay stubs or in the organizations' newsletter can keep your policy top of mind • An annual renewal of understand the policy can coincide with an employee performance review • At an annual staff meeting • By a simple organization-wide email reminder

Will you make your whistleblowing policy public?

Transparency versus public reaction

Considering to publicize your policy creates more transparency, however consider the potential for false, uninformed claims. This may include possible public reaction launched by a complainant who doesn’t understand the process or who may feel their situation has not been investigated thoroughly.

In general, situations rarely escalate to this level, but the risk is there, so consider what is best for your organization.

Who will monitor the reporting system and receive reports?

Setting up designate groups

Whether your organization is public, private or a non-profit, determining who will receive reports and lead investigations is required. You may want to set-up different groups to receive different types of report. For Example:

- Theft, fraud or other financial issues may go to the audit or finance committee
- Human resource issues may go to designates in the HR department
- Health and safety concerns may go to HR departments or a Health and Safety Coordinator.

Understanding their role and the plan

It is important that your designates understand how the reporting system works and what their responsibilities are when they receive and investigate a report. It should also be discussed when others, such as the board of directors or special investigators e.g., forensic auditor need to be brought into the process.

How will a whistleblower know if their complaint has been received and investigated if they remain anonymous?

Detail without compromising identity

It is imperative your policy stress the importance of including as much detail as possible in a report without compromising identity should the whistleblower choose to remain anonymous. Some whistleblowers will provide contact information and welcome the opportunity to provide further information, but most will rely on the information they have provided as being sufficient.

Informal meetings to discuss reported issue

The organization may consider having informal meetings for all associates to discuss the reported issue (without identifying it as a whistleblower report) to gain further insight from employees. It may lead to a follow-up report from the initial whistleblower to provide more details.

While holding these meetings will not be appropriate for all situations, it may be beneficial in certain circumstances.

Third party intermediary

If an organization uses a third party provider, they may act as an intermediary if the investigator requires additional information. When all communications go through a third part, the whistleblower maintains their anonymity while furthering the investigation.

Received, investigated and resolved

In the event a report is received, investigated and resolved, the organization may choose to inform all employees of the issue and investigation outcome. Although, this isn’t appropriate for every report, it is an option which lets employees and the whistleblower know that their system is effective.

If the report was made through an online reporting system, typically a complainant can log in and view possible communication from an organization.