

## ADM-P052 Whistleblowing Policy

*Issue Date: 2017-04-06*

*Revision Date: 2025-02-16*

*Revision #: 009*

### 1. Purpose and Scope

The purpose of this policy is to encourage persons acting in good faith, to report any suspected act of misconduct by employees, or threat to ASSL and its stakeholders and to ensure the protection of individuals who report activities believed to be illegal, dishonest, unethical, or otherwise improper.

### 2. Policy Statement

ASSL through its Code of Conduct requires employees to observe high standards of business and personal ethics in the conduct of their duties and responsibilities. Employees must practice honesty, integrity and loyalty in fulfilling their responsibilities and to comply with all applicable laws and regulations. ASSL encourages whistleblowing as a measure to protect the welfare and well-being of employees, the company and all stakeholders, providing that persons act in good faith, to report any suspected act of misconduct by employees, or risk/threat to ASSL and its stakeholders. This policy ensures the protection of individuals who report activities believed to be illegal, dishonest, unethical, or otherwise improper.

### 3. Aims and Objectives

The objectives of the ASSL Whistleblowing Policy are to establish procedures for:

- The submission of concerns regarding questionable conduct by employees, and other stakeholders of the organization, on a confidential and anonymous basis.
- The receipt, retention, and treatment of complaints received by the organization regarding acts of misconduct, internal controls, or auditing matters.
- The protection of volunteers and employees who report concerns from retaliatory actions.

### 4. Reporting Responsibility

All employees of ASSL have an obligation to report in accordance with this Whistleblowing Policy:

- a) all questionable or improper behavior or actions of co-employees, including accounting or auditing matters
- b) violations and suspected violations of ASSL policies, customer expectations or state regulations and laws.
- c) conspiracy against or threat to the organization, its employees or its stakeholders.

Typical concerns that may be raised include:

- a. Breaches of law or regulation
- b. Exploitation of customer relationships and/or standards
- c. Harassment or discrimination
- d. Employee use of drugs or alcohol
- e. Unsafe work conditions or health and safety risks

- f. Breaches of company policies, procedures or values
- g. Bribery and corruption
- h. Criminal offences, violence or threats of violence
- i. Misuse of confidential information
- j. Falsification, concealment or destruction of financial documents or accounting fraud
- k. Conflict of interest
- l. Price fixing

## **5. Anonymity and Confidentiality**

The most effective way to raise a concern is to do so openly. Openness makes it easier to assess the concern, investigate where appropriate and to obtain more information if required. However, we understand that in certain circumstances, those reporting issues of concern would like to do so anonymously and in those circumstances all concerns reported will be treated in confidence. The person's name or details will not be revealed to any party without their consent.

Whilst ASSL encourages whistleblowers to identify themselves, anonymous calls will be taken equally seriously and investigated as fully as possible. However, the effectiveness of any investigation may be limited where an individual chooses not to be identified. It is the whistleblowers decision if they choose to remain anonymous and there is never any tracking or covert attempt to discover a whistleblowers identity.

ASSL encourages anyone reporting a violation to identify himself or herself when making a report to facilitate the investigation of the violation. However, reports may be submitted anonymously by filling out a Whistleblower Reporting Form and depositing the form in a Suggestion Box located at every business location or mailing it to the CIO or appropriate recipient or calling the Telecare Hotline.

## **6. Handling Reports**

All reported concerns will be forwarded to the Chief Investigations Officer (CIO) in accordance with the procedures set forth herein. The CIO shall be responsible for investigating and making appropriate recommendations to the Chief Human Resource Officer or Chief Operations Officer with respect to all reported Concerns.

## **Whistleblower Protection**

ASSL will not retaliate against a whistleblower. This includes, but is not limited to, protection from retaliation in the form of an adverse employment action such as termination, compensation decreases, victimization or poor work assignments.

Any whistleblower who believes he/she is being retaliated against must contact the Human Resources Manager immediately. The right of a whistleblower for protection against retaliation does not include immunity for any personal wrongdoing that is alleged or proven.

This Whistleblower protection is provided in two important areas: confidentiality and retaliation. As far as possible, the confidentiality of the whistleblower will be maintained. However, there may be situations where identity may have to be disclosed to conduct a thorough investigation,

to comply with the law, and to provide accused individuals their legal rights of defense. Reports of Violations or suspected Violations will be kept confidential to the extent possible, with the understanding that confidentiality may not be maintained where identification is required by law or to enable the Organization or law enforcement to conduct an adequate investigation.

- Individuals protected include:
  - a. The employee, or a person acting on behalf of the employee, who reports to or is about to report to ASSL a matter of concern; or
  - b. The employee who participates in a court action, an investigation, a hearing, or an inquiry on a matter of concern.
- ASSL will not discharge, threaten, or otherwise discriminate against an employee regarding the employee's compensation, terms, conditions, location, or privileges of employment.

**1. The provisions of this policy do not:**

- a. require the organization to compensate an employee for participation in a court action or in an investigation, hearing, or inquiry by a public body;
- b. prohibit the organization from compensating an employee for participation in a court action or in an investigation, hearing, or inquiry by a public body;
- c. authorize the disclosure of information that is legally required to be kept confidential.

**2. Limitation to protections**

- a. A person is not entitled to the protections under this policy unless he or she reasonably believes that the information reported is a legitimate concern; and reports the information in good faith.
- b. A person is entitled to the protections under this policy only if the matter reported is not the result of conduct of the reporter (the individual seeking protection), unless it is the result of conduct by the person that was required by his or her superiors.
- c. The employee is not required to submit a written report if he or she believes with reasonable certainty that the activity, or information is an emergency or if the report is made anonymously.

## Procedures

- a. If an employee has knowledge of or a concern of illegal or dishonest/fraudulent activity or a procedural breach or conspiracy to commit any civil, company or human right violation or any other concern, the employee is to contact his/her immediate supervisor or the Chief Investigations Officer or the Chief Human Resources Officer or a senior staff member. The report can also be made via mail, the Telecare hotline, or suggestion box, or in a manner that is comfortable for the employee and in accordance with the organization incident management reporting procedure step 3.2
- b. All reports or concerns of illegal and dishonest activities must be promptly submitted by the receiving supervisor to the CIO, who is responsible for investigating and coordinating any necessary response and submit the findings to the Chief Human Resource Officer or Chief Operations Officer, for corrective action. Any concerns involving the Chief Human Resource Officer or any other member of senior management should be reported to the Chief Executive Officer.

- c. The whistleblower is not responsible for investigating the alleged illegal or dishonest activity or violation, or for determining fault or corrective measures; appropriate management officials are charged with these responsibilities.
- d. The company has no obligation to inform a whistleblower of investigation, action or outcome of any reported ill-activity.

### 3. Penalties:

- a. Any employee who violates this policy may be subject to a disciplinary inquiry that upon conviction may result in penalties outlined in the company's disciplinary procedure.

## Supplemental information

### Definitions

1. *"Whistleblower"* is defined by this policy as an employee who reports, to one or more of the parties specified in this policy, an activity that he/she considers to be illegal, dishonest, unethical, or otherwise improper.
2. *"Employee,"* means a person who performs a service for wages or other remuneration under a contract of hire, written or oral, express or implied, for the organisation.
3. *"Matter of concern"* means
  - a. a violation of a ASSL policies and procedures or state laws and, regulation, or any human rights violation;
  - b. a danger to public health or safety; and/or
  - c. Gross mismanagement, substantial waste of funds, or a clear abuse of authority.

### 4. Responsibilities of HOD's and Deputy Heads

Manager and Heads of Departments and persons acting with such or similar authority must:

1. Promote a culture of open communication within their departments where issues and concerns can easily be dealt with in the normal interaction between employees and their managers;
2. Establish internal mechanisms to manage the disclosure of wrongdoing, including – at a minimum – a designated Senior Officer, who will be responsible for receiving and acting on such disclosures. This Senior Officer will report directly to the HOD or deputy head on matters related to this policy but could also report to another manager for administrative purposes.
3. Inform all employees of this policy, including the name, location and phone number of the Senior Officer who will be responsible for receiving and acting on disclosures within their department;
4. Ensure that disclosures are reviewed in a timely fashion and forwarded to the CIO to be investigated when required, and that prompt, appropriate action is taken to correct the situation;
5. Protect the whistleblower from reprisal the employees who disclose wrongdoing in good faith.

## 5. Responsibilities of Employees

Employees are responsible for:

1. Reporting matters of concern and in good faith in accordance with their duty of loyalty;
2. Following the internal processes established to raise instances of wrongdoing or threats to the organization, its employees or stakeholders in the workplace.
3. Respecting the reputation of individuals by not making trivial or vexatious disclosures of wrongdoing or, by making disclosures in bad faith.

## 6. Responsibilities of the CIO:

1. To provide advice to employees who are considering making a disclosure;
2. To receive, record and review the disclosures of wrongdoing received from departmental employees and/or the requests for review submitted from departmental employees;
3. To establish if there are sufficient grounds for further action and review;
4. To ensure that procedures are in place to manage instances of wrongdoing that require immediate or urgent action;
5. To initiate investigation when required, to review the results of investigations and to prepare reports, and to make recommendations to deputy heads on how to address or correct the disclosure;
6. To establish adequate procedures to ensure the protection of the information and the confidential treatment of the files.
7. To protect from reprisal employees who disclose information concerning wrongdoing in good faith;

## Administrative and disciplinary measures

In respect to the application of this policy, employees and managers may be subject to administrative and disciplinary measures up to and including termination of employment, when they:

1. Retaliate against another employee who has made a disclosure in accordance with this policy or against an employee who was called as a witness; and/or
2. Choose to disclose in a manner that does not conform to this policy and its procedural requirements.

Any administrative or disciplinary measures are to be taken in consultation with the Human Resources Manager.