



# Fraud Risk Management Policy

ID #: 80-ADM-D-37

Revision Level: 0 – 17NOV2022

Created By: ABC Legal

Approved By: EVP, GC

Page 1 of 9

## Intent

---

ABC Technologies Holdings Inc., together with all of its subsidiaries and affiliates (collectively, the “**Company**” or “**ABC**”) is committed to high ethical, legal and moral standards. The Board of Directors (the “**Board**”) and the executive management (the “**Management**”) of the Company take leadership in promoting ethical behavior under the Company’s Code of Ethics and Business Conduct (the “**Code**”). All employees, vendors, consultants and contractors are expected to share this commitment and follow the Code and related policies of the Company.

This Corporate Fraud Risk Management Policy (the “**FRM Policy**”) is established to facilitate development and implementation of the Company’s Fraud Risk Management Program (the “**FRM Program**”) and related procedures and controls, including assignment of responsibility and authority for deterrence, prevention, and detection of and response to fraud against the Company.

## Policy Statement

---

Fraud or concealment of the fraud, either through the actions of the Company personnel or those working on behalf of the Company, is not tolerated at ABC.

## Scope

---

This FRM Policy applies to any fraud or suspected fraud, involving employees, Management, officers, and members of the Board as well as shareholders, consultants, vendors, contractors, outside agencies and/or any other third parties with a business relationship with the Company.

## Related Documents

---

The FRM Policy is established as a complement to other Company policies and protocols comprising, which together with the FRM Policy, comprise the *Core Policies* of the Company, and which are designed to foster and promote the highest standards of ethical business practices in the Company’s global operations.

Copies of the Company’s Core Policies can be found under the “Core Policies” section of the MyABC portal of the Company and can be requested from the members of the Company’s Human Resources and Legal departments.

## Actions Constituting Fraud

---

Fraud includes but is not limited to the following examples, which can be categorized as falling into one of four main categories:

1. Fraudulent Financial Reporting:
  - a. Improper revenue recognition (over or under-statement);
  - b. Improper expense or liability recognition;
  - c. Improper asset valuation (generally overstated);
  - d. Improper disclosures;
  - e. Manipulation of models, budgets or results.
  
2. Fraudulent Non-Financial Reporting:
  - a. Corporate or individual qualifications and performance;
  - b. Program (launch) status and performance;
  - c. Vendor qualifications and performance;
  - d. Quality reporting (OEM, ISO, etc.);
  - e. Compliance reporting (environment, H&S, UN Global Compact, etc.).
  
3. Asset Misappropriation:
  - a. Theft of or damage to assets;
  - b. Employee asset misuse or diversion;
  - c. Employee compensation schemes;
  - d. Credit or cheque and collection schemes;
  - e. Cyber attacks.
  
4. Other Illegal Acts and Corruption:
  - a. Operating without environmental permits or approvals;
  - b. Legislative non-compliance (labour laws, trade laws, etc.);
  - c. Improper relationships (government, conflicts of interest, vendors);
  - d. Improper expenditures (facilitation payments, bribes, kick-backs);
  - e. Aiding or abetting third parties (bid-rigging, price fixing).

A fraudulent act remains fraudulent even if it does not result in a significant financial loss to the Company. Even seemingly small acts such as those in the following examples are fraudulent acts, unless they are taken in the circumstances clearly permitted by the Company's policies:

- a. Taking the office stationery home for personal use;
- b. Using the office computer or telephone for personal use;
- c. Recording personal time as office time.

## **Roles and Responsibilities**

---

All personnel, regardless of their level, have a responsibility to help the Company deter and defend against fraud. The section below highlights the roles and responsibilities of the Board and its Audit Committee, Management, Legal Department, Human Resources Department, Assurance & Advisory Services department ("**Internal Audit**") and other employees in respect of the FRM Program.

## **Board and Audit Committee**

The Board through its Audit Committee is responsible for setting the tone for the Company and to ensure that Management has implemented an effective FRM Program by:

- Understanding and discussing fraud and corruption risks that could impact the Company;
- Reviewing the FRM Policy;
- Approving fraud risk tolerances;
- Overseeing the FRM Program, including Management's:
  - fraud risk assessment;
  - reports on fraud risks and controls;
  - investigation of and response to fraud allegations;
  - evaluation of the FRM Program;
  - supporting Internal Audit's annual plan and ensuring their accessibility to information, books, records, and employees.

## **Management**

Management has overall responsibility for the design and implementation of the FRM Program, including:

- Assigning the overall responsibility for the FRM Program, including implementation of the FRM Policy and reporting to the Audit Committee on the FRM Program activities;
- Ensuring that fraud risk is addressed in the Company's strategic objectives and risk assessment activities;
- Implementing the processes and controls to deter, prevent and detect fraud;
- Developing training and awareness activities to promote understanding among employees about the FRM Policy and other Core Policies;
- Maintaining an open-door policy and other channels for reporting potential fraud concerns or complaints;
- Supporting and working with Internal Audit, Company's external auditors and, if required, law enforcement agencies in detection, reporting and investigation of suspected fraudulent activities;
- Monitoring successful completion of corrective action against fraud incidents and remediation of controls as required;
- Monitoring and evaluating the FRM Program periodically or on an *ad hoc* basis, should a change in the fraud risk environment occur, such as, change in

operations, merger/acquisition, identification of a fraud event etc., and modifying the fraud control processes and activities as required.

### **Legal Department**

The Company's General Counsel is the head of the Legal Department of the Company and is responsible for the FRM Policy, leading the FRM Program and fraud risk management activities under the direction of the Audit Committee and Management, including:

- Developing the core elements of the FRM Program, policies, and procedures;
- Developing the procedures for escalation, assessment, investigation, and closure of allegations of fraud;
- Leading fraud risk assessment and design and implementation of controls for deterrence, prevention and detection of fraud;
- Managing assessment and investigation of allegations involving fraud and engaging outside counsel and reporting to law enforcement as required;
- Managing civil/criminal litigation and asset recovery proceedings;
- Answering (either directly or through other members of the Legal Department) questions about ethics-related matters;
- Providing periodic reports to Audit Committee and Management on the FRM Program status, including litigation and asset recovery.

### **Human Resources**

The Human Resources department is responsible for the key anti-fraud procedures relating to employees' conduct for compliance with the Code and the FRM Policy, including through the following:

- Screening employee candidates and conducting, where appropriate, and in accordance with the Company's Background Check Policy, background checks;
- Facilitating new hire and refresher training relating to the FRM Policy, other Core Policies and other compliance matters;
- Participating in fraud risk assessment;
- Conducting annual employee surveys, including employee satisfaction and awareness;
- Reviewing and escalating potential fraud related complaints;
- Conducting exit interviews to identify, among others, concerns involving potential fraud;
- Supporting internal/regulatory fraud investigations;

- Facilitating administration of disciplinary/corrective action.

## **Employees**

Strong controls against fraud are the responsibility of everyone in the Company. All employees must:

- Have a basic understanding of fraud, be aware of red flags and be alert for any indications of fraud;
- Read, understand, and affirm the FRM Policy and other Core Policies;
- Understand their roles in the internal control framework and participate in design and implementation of anti-fraud control activities;
- Report concerns, suspicions, and incidents of fraud;
- Cooperate in investigations.

## **Internal Audit**

The Company's Internal Audit department provides independent, objective assurance regarding the design and operating effectiveness of management's anti-fraud controls, including through the following:

- Incorporating fraud risk review in the annual audit plan;
- Reviewing the organization's anti-fraud culture, the Board and Audit Committee's oversight activities and Management's participation in fraud risk assessment and anti-fraud controls;
- Evaluating Management's fraud risk assessment and effectiveness of the anti-fraud controls through walk-throughs and testing, as applicable;
- Reporting to Audit Committee and Management on the evaluation of the FRM Program including design and operating effectiveness of anti-fraud controls;
- Assisting in investigations, as required, and reporting to the Audit Committee on related matters.

## **Fraud Risk Assessment**

---

The Company is committed to the timely prevention and detection of fraud. Management will conduct periodic fraud risk assessments for the purpose of identifying, analyzing, and responding to key fraud risks across the Company.

The fraud risk assessment process will consider key factors that drive fraud, namely, opportunities, incentives and pressures, and attitudes and rationalization and will address the four key types of fraud, as detailed in Section "Actions Constituting Fraud" above.

The risk assessment methodology will consist of:

- Identifying entity and process level fraud risks using common fraud scenarios;
- Prioritizing the significance and likelihood of such risks on inherent and residual basis through a series of interviews with Management and employees selected from a variety of departments, geographic locations, and management levels within the Company;
- Mapping fraud risks to existing internal controls; and
- Identifying potential gaps or enhancement opportunities related to anti-fraud control activities.

The results of Management's fraud risk assessment will be addressed in an action plan and reported to the Audit Committee. The results and the action plan will be considered by Internal Audit in the internal annual audit plan.

## **Anti-fraud Controls**

---

Management has designed a combination of preventive and detective anti-fraud control activities which operate at various levels of the Company and are intended to facilitate timely detection of fraud events and to help mitigate the occurrence of fraud.

High-level fraud prevention control activities include:

- Business and Human Resources control activities, such as authority and responsibility matrix, segregation of duties, employee screening and background checks, training, employee surveys and exit interviews;
- Transaction control activities, such as managerial review and approval, matching vendor invoice with purchase order and material receiving report;
- Physical access control activities, such as access rights to the Company's facilities and right to use inventory, computer systems;
- Technological controls activities, such as logical access rights to sensitive information and applications on the Company's information systems.

High-level fraud detection control activities include:

- Review and reconciliation control activities, such as bank reconciliation, inventory reconciliation, performance reports;
- Data analytics performed by operations, and finance/accounting departments to continuously monitor certain types of processes, transactions, and payments;
- Reporting mechanisms and channels to receive, analyze and treat information, concerns, and complaints about potential fraud,

## **Fraud Reporting, Investigation and Corrective Action**

---

### **Fraud Reporting**

The Company's Code requires employees, Management, and the Board to report all incidents of fraud.

The primary method of reporting fraud is by submitting a whistleblowing report to the **EthicsPoint Hotline**, which is maintained for the Company by NAVEX, an independent third party-service provider.

Submissions of reports to the EthicsPoint Hotline may be made online at **abcgrp.ethicspoint.com** and by telephone in local languages of all jurisdictions in which the Company conducts business.

The telephone dialing instructions for reaching the EthicsPoint Hotline can be found in appendixes to the Code and the Company's Whistleblowing Policy and are otherwise periodically communicated to employees.

Additional channels available to employees and others for reporting fraud include:

- Discussion with or email to Supervisor for any matter;
- Discussion with or email to Human Resources for any matter;
- Discussion with or email to Legal Department for any matter;
- Letter or email to General Counsel for any matter;
- Letter or email to Head of Internal Audit for any matter;
- Letter or email to any member of Management for any matter;
- Letter or email to the Chair of the Board/Audit Committee for any accounting, internal controls, or auditing matters;
- Letter or email to the Chair of the Board/Audit Committee for any matters involving any member of the Management.

Customers, vendors and other third parties are encouraged to report fraud through the EthicsPoint Hotline or to communicate by letter or email with the Company's General Counsel at [Ryan.Conacher@abctech.com](mailto:Ryan.Conacher@abctech.com).

Reports provided to the Company about fraud, including the reports made through the EthicsPoint Hotline, can be anonymous. In other cases, confidentiality of the report and the reporter will be maintained to the fullest extent possible. The Company's Board and Management underscore a work environment that is free from retaliation, as is expressly stated in the Code. Swift and appropriate action will be taken in cases of retaliation.

*Any employee may report a good faith concern or potential violation involving fraud without fear of dismissal or retaliation.*

### Fraud Investigation and Corrective Action

The Legal Department has established investigation protocols for conducting all investigations which are followed to review, analyze and treat the reports relating fraud.

Supervisory personnel, as well as the Legal and Human Resources Departments, who receive a report relating to a concern or a complaint about fraud are required to immediately report the event through the EthicsPoint Hotline or otherwise report the events to the General Counsel. Upon receipt of a report related to actual or suspected fraud through the EthicsPoint Hotline, or as otherwise reported to the General Counsel, the matter in the report will be reviewed by the General Counsel, or his designee, to determine the nature and appropriate treatment of the concern or complaint. The Legal Department will keep appropriate records of the report.

If an investigation is warranted, the General Counsel or his designee will take steps to:

- Assign internal resources, and if appropriate consult with the CEO or other members of Management, if external counsel or consultants will be required, to conduct the investigation;
- Notify employees regarding document preservation and securing data systems, considering privacy and other relevant laws and regulations;
- Consider the requirement to notify the regulators, law enforcement and other third parties, such as external auditors and insurance companies;
- Develop an investigation plan;
- Conduct the investigation while protecting confidentiality and safeguarding evidence;
- Adhere to policies regarding retention of evidence and other documents, working papers and reports;
- Report the results of the investigation to Board/Audit Committee, Management, external auditors, Internal Audit etc.;
- Assess the root causes and commence remediation, in conjunction with Human Resources Department and Internal Audit;
- Assist as required, based on the facts confirmed in investigation results, the respective Department Head and Human Resources in disciplinary, termination and asset recovery actions;
- Contact the reporter of the matter, concern or complaint, if appropriate, to share high-level investigation results;
- Review and assess investigation performance for future improvements in the suspected fraud investigation protocols.





## Fraud Risk Management Policy

ID #: 80-ADM-D-37

Revision Level: 0 – 17NOV2022

Created By: ABC Legal

Approved By: EVP, GC

Page 9 of 9

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

### **FRM Program Monitoring and Evaluation**

---

All the components of the FRM Program will be evaluated during management's periodic fraud risk assessment, or on an *ad hoc* basis, should a change in the fraud risk environment occur. The operating effectiveness of the related anti-fraud controls will be tested by the Internal Audit during their ongoing audits under the annual audit plan.

Periodically, Internal Audit will conduct a separate and independent evaluation of the FRM Program. Internal Audit will report the findings to the Board/Audit Committee and Management. The General Counsel is responsible for ensuring that any deficiencies involving anti-fraud control activities are addressed in timely and effective manner.

This FRM Policy will be assessed by the General Counsel and reviewed by the Management and the Audit Committee on a periodic basis. Any changes to the Policy will be communicated to the employees and relevant third parties in a timely manner.

