APPENDIX F4: SAMPLE FRAUD RISK MANAGEMENT POLICY

This sample policy can be adapted to meet the needs and revised to match the structure of a particular organization.

1. Policy Statement

ABC Company ("Company") is committed to ethical business practices within its worldwide operations. Under no circumstances is management tolerant of fraud and misconduct, either through the actions of its personnel or those working on its behalf.

The *Fraud Risk Management Policy* ("Policy") establishes management's framework of internal controls for the prevention and detection of fraud and misconduct (collectively, "Fraud Risk Management Program") within the Company, as well as protocols for conducting internal investigations.

This Policy applies to any fraud or misconduct, or suspected fraud and misconduct, involving employees as well as the Board of Directors ("Board"), management, and third parties with a business relationship with the Company. Any employee may submit a good faith concern or potential violation involving fraud without fear of dismissal or retaliation. Investigations will be conducted without regard to suspected personnel or third party's length of service, position/title, or relationship to the Company. Disposition of matters, as well as decisions to prosecute or refer to regulatory agencies and/or law enforcement will be made in conjunction with the legal department, management, and the board of directors, as appropriate.

2. Definitions

Fraud is defined as any intentional act or omission designed to deceive others, resulting in the Company suffering a loss and/or the perpetrator achieving a gain. Management personnel are expected to be familiar with the types of fraud that could occur within their specific areas of responsibility and report any suspected or known instances of fraud within the Company.

Misconduct is defined as any intentional violation, or suspected violation, of the Company's policies and procedures, as well as applicable laws and regulations with which the Company must comply.

Retaliation is defined as any direct or indirect detrimental action recommended, threatened or taken, because an individual provided a good faith report of fraud or misconduct to the Company or cooperated in assigned fact-finding activites.

3. Fraud Control Strategy

A. **Roles and Responsibilities**

All personnel, regardless of their level, are responsible for helping deter and defend the Company from fraud and misconduct. Certain management and employees have specific anti-fraud control responsibilities which are further defined within job descriptions, department charters and/or other Company policies. The section below highlights the roles and responsibilities of the board and audit committee, management, legal department, human resources department and employees within the Company's Fraud Risk Management Program:

Board and Audit Committee

To set the appropriate tone for the Company, the Board is responsible for ensuring that management designs an effective Fraud Risk Management Program by:

- Understanding and discussing fraud and corruption risks that could impact the Company;
- Establishing independent board processes and practices;
- Developing the chief executive officer's job description and overseeing evaluations and succession planning processes;
- Periodically reviewing management's *Fraud Risk Management Policy*, as well as other applicable Company policies and procedures designed to help mitigate fraud risk;
- Ensuring that fraud risk has been considered as part of management's strategic objectives and risk assessment activities;
- Overseeing management's fraud risk assessment activities;
- Assessing the risk of fraud by management, including the risk of management's override of controls, and ensuring that controls are designed and functioning to deter, prevent, and detect fraud by management;
- Monitoring management's reports on fraud risks, policies, and control activities;
- Supporting the internal audit department's annual plan and ensuring accessibility to information, data, and employees;
- Ensuring that the internal audit department has unrestricted access to the board and its internal audit committee;
- Ensuring that all employees have access to the board, audit committee, and internal audit department;
- Empowering the audit committee to focus on fraud deterrence, prevention, and detection;
- Being fully informed about instances of fraud that occur within the organization, in particular, instances involving senior-level employees or employees about whom significant internal control issues are uncovered;
- Ensuring that management has assigned sufficient resources to execute fraud risk management activities; and
- Retaining outside advisors and counsel, as necessary.

Management

Management has overall responsibility for the design and implementation of the Company's fraud risk management program, including:

- Ensuring that fraud is addressed in the Company's strategic objectives and risk assessment activities;
- Appointing the fraud control officer, who has overall responsibility for the coordination and implementation of the Company's fraud risk management program, as well as reporting to the Board about fraud risk matters;
- Identifying and assigning personnel responsible for anti-fraud control activities and maintaining

records that verify that those processes and controls have been properly executed;

- Providing defined, proactive processes and control activities to deter, prevent, and detect fraud;
- Implementing internal controls designed to prevent and/or detect fraud within each business unit;
- Developing training and awareness activities to promote understanding and compliance with the *Code of Conduct*, *Fraud Control Policy*, *Whistleblower and Anti-Retaliation Policy, Conflicts of Interest Policy and Disclosure Form, Anti-Corruption Compliance Policy* and other corporate policies;
- Maintaining an open-door policy and other mechanisms to report fraud and misconduct; and
- Monitoring the successful completion of disciplinary and corrective action, when assigned.

<u>Legal Department</u>

The Legal Department advises management on the legal ramifications of the fraud risk management program, which includes:

- Participating in the creation of key Company policies and procedures;
- Guiding the escalation, assessment, investigation and closure of allegations involving fraud and misconduct;
- Participating in the flow of information about investigations to senior management and the audit committee, as well as regulators and law enforcement, as appropriate;
- Assisting in the recovery of lost assets due to fraud and misconduct;
- Analyzing case management activities pertaining to matters involving fraud and misconduct;
- Providing communication regarding litigation and other asset recovery efforts on a periodic basis to the audit committee;
- Managing fraud prevention and detection control activities, as assigned;
- Answering questions about ethics-related matters;
- Participating in management's fraud risk assessment, as well as fraud risk awareness and training activities; and
- Implementing, tracking and communicating new legislative and regulatory requirements.

<u>Human Resources</u>

The human resources department assists management and employees by executing key anti-fraud control activities through on-boarding, training, counseling, and issue resolution activities and processes, including:

- Screening of employee candidates and periodic updates to employee background investigations;
- Facilitating new employee orientation and other employee training activities, which includes the annual review and affirmation of key corporate policies such as the *Code of Conduct*, *Fraud Control Policy, Whistleblower and Anti-Retaliation Policy, Conflicts of Interest Policy and Disclosure Form,* and *Anti-Corruption Compliance Policy*;
- Conducting, analyzing and reporting on the results of employee satisfaction and fraud awareness surveys;

- Escalating issues involving potential fraud and misconduct reported by management and employees;
- Participating in management's fraud risk assessment activities;
- Providing management and the internal audit department with information about employee hires and departures;
- Reviewing resignation letters and conducting exit interviews in order to identify and escalate any potential concerns or complaints involving fraud and misconduct;
- Supporting internal investigation activities, as needed;
- Monitoring the disposition of disciplinary or correction action, when administered;

Internal Audit

The internal audit department provides independent, objective assurance regarding the design and operating effectiveness of management's anti-fraud controls, including:

- Evaluating the potential for the occurrence of fraud and how the Company manages fraud risk through walk-throughs and review of the Company's fraud risk management program;
- Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls commensurate with the extent of the potential exposure/risk in various segments of the Company's operations;
- Ensuring that management has reviewed its risk exposure and identified the possibility of fraud as a business risk through a fraud risk assessment;
- Incorporating information about fraud obtained through the fraud risk assessment process, reporting mechanisms and investigations with the annual internal audit plan;
- Delivering information to the audit committee about the adequacy of management's arrangements for mitigating fraud risk and ensuring that the Company promotes an anti-fraud culture; and
- Assisting in investigations and reporting of matters to the Audit Committee.

Employees

Strong controls against fraud are the responsibility of everyone in the organization. All levels of personnel within the Company will:

- Have a basic understanding of fraud, be aware of red flags, be familiar with the types of fraud that might occur within their areas of responsibility, and be alert for any indications of fraud;
- Understand their roles within the internal control framework. Personnel must understand how their job procedures are designed to manage fraud risks and when noncompliance may create an opportunity for fraud to occur or go undetected;
- Read, understand and affirm Company policies and procedures designed to mitigate fraud and misconduct (e.g. *Fraud Control Policy*, *Code of Conduct*, *Whistleblower and Anti-Retaliation Policy, Conflicts of Interest Policy and Disclosure Form, Anti-Corruption Compliance Policy,* etc.);
- As required, participate in the process of creating a strong control environment and designing and implementing fraud control activities, as well as participate in monitoring activities;
- Report concerns, suspicions or incidences of fraud; and
- Cooperate in investigations.

B. **Fraud Risk Management Program**

The Company's fraud risk management program ("Program") is administered by the fraud control officer, ______________________________, who reports to the board on matters involving fraud risk. The Program reflects the concepts of governance, risk assessment, fraud prevention and detection, investigations and corrective action, and monitoring.

Each component of the Program is designed to help mitigate potential fraud and misconduct identified during management's fraud risk assessment. Each component is documented within this Policy and periodically updated to reflect the evolving nature of fraud risk within the Company's operations.

C. **Relationship to Code of Conduct and Other Company Policies**

The board and management have adopted the *Fraud Control Policy* as a complement to other company policies designed to foster and promote the highest standards of ethical business practices amongst the Company's global operations. Personnel at every level have responsibility for ensuring that the Company's business activities align with the *Code of Conduct*, as well as other policies designed to ensure compliance with laws, rules, and regulations in the jurisdictions in which the Company operates. These include the following:

- *Code of Conduct*
- *Whistleblower and Anti-Retaliation Policy*
- *Conflicts of Interest Policy and Disclosure Form*
- *Anti-Corruption Compliance Policy*

Each policy is available to employees through the Company intranet located at _________________. Copies of these Company policies are available on the Company's Internet site and have been provided to certain third parties as part of the contracting process.

4. Fraud Risk Assessment

The Company is committed to the timely prevention and detection of fraud and misconduct. Management, with the assistance of the internal audit department, conducts an annual fraud risk assessment for the purpose of identifying, analyzing and responding to key fraud risk across all of its geographic locations.

The fraud risk assessment process considers key factors that drive fraud – opportunities, incentives and pressures, and attitudes and rationalization. It also addresses four (4) key types of fraud – corruption, asset misappropriation, fraudulent reporting and management override of controls. The risk assessment methodology consists of identifying entity and process-level fraud risks utilizing common fraud scenarios; prioritizing the significance and likelihood of such risks on an inherent and residual basis through a series of interviews with management and employees selected from a variety of departments, geographic locations and professional levels within the Company; mapping fraud risks to internal controls; and identifying potential gaps or enhancement opportunities related to management's anti-fraud control activities. The results of management's fraud risk assessment are addressed within an action plan, incorporated within the internal audit department's annual plan and shared with the Board.

5. Fraud Prevention and Detection Controls

Management has designed a combination of preventive and detective anti-fraud control activities which occur at various levels of the Company and are intended to help mitigate the occurrence of fraud and misconduct, as well as ensure the timely detection of fraud risk events within business operations.

The Company's high-level fraud prevention control activities include:

- Business process control activities include the use of authority and responsibility limits, as well as human resource procedures such as employee background investigations, training, employee surveys, and exit interviews.
- Physical access control activities address admittance to the Company's facilities and right to use of assets, such as inventory.
- Logical access control activities address access rights to sensitive information.
- Transaction control activities address procurement procedures and managerial approval requirements.
- Technological control activities include electronic third party screening activities and automated restrictions on certain payments that present elevated risk to the Company or do not comply with prescribed Company policy requirements.

The Company's high-level fraud detection control activities include:

- Data analytics (both overt and covert) utilized by the finance and accounting department to continuously monitor certain types of payments and transactions, as well as data analytics used by the internal audit department in its performance of operational and financial audits.
- Multiple automated and manual reporting mechanisms created by the board and implemented by management to receive, retain and treat concerns, complaints and information about potential violations of fraud and misconduct across the Company's business operations.

6. Fraud Reporting

The Company has a "speak up" culture and requires employees, management and the board to report all incidents of fraud and misconduct. The Company has established an ethics hotline (_________________________) and corresponding Internet site (_______________________) which are available on a 24 hour, 7 day per week and 365 day per year basis in _________________, ________________, __________________ and ______________ languages for the purpose of receiving concerns, complaints and information about fraud and misconduct. Additional channels available to employees and others for reporting fraud and misconduct include:

- Sending a letter to the board, legal department or fraud control officer at ______________________;
- Sending electronic mail ("email") to the fraud control officer at ___________________________;
- Discussion matters with supervisory personnel; and

- Direct and open communications with members of the human resources or legal departments.

Furthermore, third parties are encouraged to report fraud and misconduct impacting the Company either through the ethics hotline, internet site or corresponding to the board, legal department or fraud control officer. Such information is made public on the Company's website at _____________________________ and/or provided to third parties during contracting activities.

Reports provided to the Company about fraud and misconduct can be anonymous if they are made through the ethics hotline, internet site, or written correspondence. Otherwise, confidentiality will be maintained to the fullest extent possible. The Company fosters a work environment free from retaliation and takes swift and appropriate action in cases in which retaliation may occur. Additional information about the reporting of fraud and misconduct is provided in the Company's *Whistleblower and Anti-Retaliation Policy*.

7. Fraud Investigation Procedures

Upon receipt of a report, the matter will be evaluated by the Company's legal department, in conjunction with the fraud control officer, to determine the nature and treatment of the complaint in accordance with the procedures established by the board and as outlined in the Company's *Code of Conduct* and *Whistleblower and Anti-Retaliation Policy*. Supervisory personnel, as well as those in the human resource and legal departments who receive a report of fraud or misconduct, are required to immediately report the event through the ethics hotline. The legal department will record the report, along with information about the disposition of the matter, in the Company's case management log.

If an investigation is warranted, the legal department will take steps to:

- Assign internal resources and consult with the board regarding the need to retain external counsel or consultants in order to conduct the investigation;
- Consider requirements for notification to regulators, law enforcement and other third parties, such as the Company's external auditors and insurance company;
- Notify employees regarding document preservation and securing data systems, considering data privacy and other pertinent laws and regulations in the jurisdiction(s) where the investigation will occur;
- Develop an investigation work plan;
- Conduct the investigation while protecting confidentiality or anonymity and safeguarding evidence;
- Report the results of the investigation to the board, fraud control officer, and others as appropriate (e.g., management, external auditors, etc.);
- Adhere to policies regarding retention of reports, documents, work papers, and other information;
- Assess root causes and commence remediation and corrective action in conjunction with the fraud control officer, as well as the human resource and internal audit departments.
- Commence disciplinary, termination, asset recovery, and restitution actions in conjunction with the fraud control officer and human resource department based upon the facts confirmed during the investigation.
- Contact the reporter of the matter, complaint, or violation, if appropriate, to share high-level

investigation results and obtain feedback about the investigation process.

- Conduct case analysis to assess investigation performance and enhance future investigation procedures.

Investigation resources will be provided with unrestricted access to all Company records and premises, whether owned or rented. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Performance metrics for investigations may vary and can include the average number of days to evaluate and resolve an issue, as well as internal resource hours, costs associated with external assistance, type(s) of remediation and corrective action, and repeated number of incidents involving either an individual, department, or geographic location.

8. Fraud Monitoring Activity

The design of the components within the fraud risk management program will be evaluated during management's annual fraud risk assessment, or sooner, should a fraud risk event occur. The operating effectiveness of related anti-fraud controls will be tested annually as part of management's Sarbanes-Oxley ("SOX") compliance activities.

Periodically, the internal audit department will conduct a separate and independent evaluation of the fraud risk management program utilizing authoritative guidance and leading practices. Internal audit will report its findings to the board and management. The fraud control officer is responsible for ensuring that any deficiencies, weaknesses, or enhancements involving anti-fraud controls are addressed in a timely and effective manner. In addition, internal audit activity will consider the risk of fraud and misconduct as part of its financial and operational audits conducted throughout the course of the year.

This Policy will be assessed by management and reviewed by the Company's board on a periodic basis and no less than every two (2) years. Any changes to the Policy will be communicated to Company personnel and relevant third parties in a timely manner.

APPROVED: ____

(Chief Executive Officer) Date

RATIFIED: ____

(Chairperson, Board of Directors) Date

IMPLEMENTED: ____

(Fraud Control Officer) Date