SEMICONDUCTOR MANUFACTURING INTERNATIONAL CORPORATION

ANTI-FRAUD POLICY

INTRODUCTION

This policy covers the prevention, detection, control and investigation of fraud and for fair dealing in investigations of alleged fraud.

It aims to raise the awareness of fraud and its prevention and to give guidance to both the reporting of suspected fraud and how the investigation of that report will proceed.

1. Policy

1.1 Policy Statement

Semiconductor Manufacturing International Corporation ("**SMIC**") is dedicated to the prevention, detection, control and investigation of fraud and to fair dealing when investigating allegations of fraud.

1.2 Policy Objectives

- To ensure that management is aware of its responsibilities for identifying fraudulent activities and for establishing controls and procedures for preventing such fraudulent activity and/or detecting such fraudulent activity when it occurs.
- To provide guidance to employees as to action which should be taken where they suspect any fraudulent activity.
- To provide a clear statement to staff forbidding any illegal activity, including fraud for the benefit of SMIC.
- To provide clear guidance as to responsibilities for conducting investigations into fraudulent activities.
- To provide assurances that any and all suspected fraudulent activity will be fully investigated.
- To provide a suitable environment and adequate protection and guidance for employees to report matters that they suspect may concern corrupt conduct, criminal conduct, criminal involvement or serious improper conduct

1.3 Definitions

Fraud is a broad concept that refers to any intentional act committed to secure an unfair or unlawful gain, which includes, among other things, (a) allegations of fraud, misconduct or errors related to SMIC's accounting or financial reporting systems, controls or disclosures; and (b) allegations of securities law violations (*e.g.*, insider trading or disclosure issues) and commodities law violations.

Financial fraud typically falls into four broad categories:

- Fraudulent financial reporting – Most fraudulent financial reporting schemes involve earnings management, arising from improper revenue recognition, and overstatement of assets or understatement of liabilities.
- Misappropriation of assets - This category involves external and internal schemes, such as embezzlement, payroll fraud and theft.
- Expenditure and liabilities for improper purposes –This category refers to commercial and public bribery, as well as other improper payment schemes.
- Fraudulently obtained revenue and assets, and costs and expenses avoided - This category refers to schemes where an entity commits a fraud against its employees or third parties, or when an entity improperly avoids an expense, such as tax fraud.

1.4 Strategies

SMIC has adopted a holistic approach to prevent and to detect fraud. Every employee is trained to abide by the ethics standards set out in the Code of Business Conduct and Ethics.

SMIC's management is responsible for designing, monitoring, and evaluating the company's anti-fraud control mechanisms. Every employee is responsible for reporting suspected fraud cases. The procedures for reporting and investigating alleged fraud cases are outlined in Section 3 of this policy.

Management will conduct an annual self-assessment of the design and operating effectiveness of SMIC's anti-fraud programs. This assessment will be conducted under the framework for evaluating internal controls developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The COSO framework views internal controls as consisting of the following five interrelated components:

- Control Environment: the integrity and ethical values of the company, including its code of conduct, involvement of the Board of Directors and other actions that set the tone of the organization
- Risk Assessment: management's process of identifying potential risks that could result in misstated financial statements and developing actions to address those risks
- Control Activities: these are the activities usually thought of as the "internal controls"; they include such things as segregation of duties, account reconciliations and information processing controls that are designed to safeguard assets and enable an organization to timely prepare reliable financial statements;
- Information and Communication: the internal and external reporting process and includes and assessment of the technology environment

- Monitoring: assessing the quality of a company's internal control over time and taking actions as necessary to ensure it continues to address the risks of the organization

The Risk Management Committee and the Audit Committee shall review the results of the self-assessment.

In addition to this policy, the associated policies and documents at SMIC for the prevention, detection, control and reporting of fraud and corrupt conduct have several other elements, including:

- Codes of Business Conduct and Ethics
- Human Resources Policies and Procedures Manual
- Accounting and Finance Policies and Procedures Manual
- Internal Audit Charter
- Risk assessment procedures
- Ethics Hotline
- Oversight by Audit Committee/Board of Directors ("Board")
- Compliance Office Standard Operating Procedures ("Compliance Office SOP")
- Insider Trading Policy
- SMIC Classified Information Protection Policy (CIPP)
- Gift Policy

2. Guidelines

2.1 Responsible Parties

The Audit Committee, with the support of the Risk Management Committee and the Compliance Office, is responsible for the oversight of the control and administration of this policy.

2.2 Responsibilities for Implementation of This Policy

The Audit Committee, with the support of the Risk Management Committee and the Compliance Office, is responsible for overseeing that appropriate and effective internal control systems are in place.

The Chief Compliance Officer monitors and implements this policy and investigates any fraud issues reported to the Compliance Office.

The Risk Management Committee will ensure that SMIC has a system in place for identifying and evaluating risk, control and measures to improve/optimize the

organization's risk profile and key performance indicators and communication techniques that apply across and upwards through the organization.

The Internal Audit Office supports the chairman of the Risk Management Committee in ensuring appropriate and effective internal control systems are operating.

It is the responsibility of all managers to ensure that there are mechanisms in place within their area of control to:

- Assess the risk of fraud;
- Determine which control prevents and detects fraud;
- Determine who will perform the controls and the related segregation of duties;
- Assess the effectiveness of anti-fraud programs;
- Promote employee awareness of ethical principles to which SMIC adheres; and
- Educate employees about fraud prevention and detection.

For this purpose, the managers should incorporate into their annual planning processes, fraud control plans covering risk assessment, awareness programs and training.

2.3 Ethics Hotline

All employees also have the responsibility to report suspected fraud. Any employee who suspects fraudulent activity must immediately notify the Compliance Office (at Code@SMICS.com) and/or the Audit Committee (at AuditCommittee@SMICS.com). Reports may be submitted anonymously if the employee desires.

2.4 Recruitment of Staff

When recruiting new staff, Human Recourses must:

- Perform criminal background checks, where the roles and responsibilities of the position warrants such checks;
- Contact previous employers and/or references, and
- Verify transcripts, qualifications, publications and other certification or documentation.

2.5 Staff Development and Training

Courses and seminars on the topic of fraud, fraud detection and fraud prevention will also be developed by the Human Resources Department and Compliance Office, with assistance from Internal Audit, as necessary. Employees must attend these courses and seminars when requested by the Human Resources Department and Compliance Office.

2.6 Review of Policy and Effective Date

In the interests of maintaining best practice, the Compliance Office shall review this policy on an annual basis. The outcome of the review shall be reported to the Chairman of the Risk Management Committee, the Audit Committee and the Board. Any amendments to this policy shall come into effect immediately upon approval by the Board.

3. ADMINISTRATIVE PROCEDURES

3.1 Investigations of Complaints

Any complaints concerning suspected fraud of supervisors shall be reported to the Compliance Office and/or the Audit Committee directly, and

3.1.1 Investigation of alleged Fraud relating to Financial Reporting and Cases Involving Executive Officers or the Chief Compliance Officer

The Chief Compliance Officer shall bring all alleged fraud cases relating to financial reporting and all cases involving the Company's executive officers or the Chief Compliance Officer directly to the Audit Committee in accordance with the Compliance Office SOP. The Audit Committee shall assume the responsibility of investigating frauds relating to financial reporting and cases involving the Company's executive officers or the Chief Compliance Officer.

3.1.2 Investigation of alleged Fraud not relating to Financial Reporting and Not Involving Executive Officers or the Chief Compliance Officer

The Chief Compliance Officer will initially conduct a preliminary fact finding review on alleged fraud cases not relating to financial reporting and not involving the Company's executive officers or the Chief Compliance Officer.

After the preliminary review of the complaint, the Chief Compliance Officer may request assistance from the relevant departments, outside counsels and other appropriate parties inside and outside the organization as to the validity1(d)-6( )]TJETBT1

- Avoidance of any unnecessary litigation.

Employees must co-operate fully with law enforcement and regulatory agencies, including reporting to such agencies and support of prosecution, where necessary.

4. Confidentiality

All cases reported must be treated with strict confidence at all stages and be dealt with in accordance with the Compliance Office SOP.

In order to avoid damaging the reputations of innocent persons initially suspected of wrongful conduct, and to protect SMIC from potential civil liability, the results of the audits/investigations will be only be disclosed to, or discussed with, those persons and external advisers of the Company who require the knowledge in the proper performance of their office or function. All the investigation reports, complaints or the identities of the persons involved shall be kept highly confidential and in accordance with the Compliance Office SOP.

5. No Retaliation

SMIC encourages individuals to in good faith report suspected fraud and cooperate in the investigation of reported violations. SMIC will not discharge, demote, suspend, threaten, harass or in any other manner discriminate or retaliate against any employee because of communications made in good faith under this Policy. Any act of retaliation should be reported immediately and will be disciplined appropriately. This Policy is intended to encourage and enable employees and others to in good faith raise serious concerns within SMIC prior to seeking resolution outside SMIC.

However, employees who file reports or provide evidence which they know to be false or without a reasonable belief in the truth and accuracy of such information will not be protected by the above policy statement and may be subject to disciplinary action, including termination.