1. OBJECTIVE

The corporate fraud policy is established to facilitate the development of controls that will aid in the detection and prevention of fraud against ***Panasonic Manufacturing Philippines Corporation (PMPC, the "Company").*** It is the intent of PMPC to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigations. ***Appendix A*** summarizes the Company's Fraud Policy Framework to effectively mitigate the incident of fraud.

2. SCOPE OF POLICY

2.1. This policy applies to any irregularity, or suspected irregularity, involving employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with PMPC (also called the Company).

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

3. POLICY

3.1. Management is responsible for the detection and prevention of fraud, misappropriations, and other irregularities. Fraud is defined as the intentional, false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury. Each member of the management team will be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity.

3.2. Any irregularity that is detected or suspected must be reported immediately to the Director of Finance, who coordinates all investigations with the Legal Department and other affected areas, both internal and external.

4. CONSTITUITNG FRAUD

4.1. The terms defalcation, misappropriation, and other fiscal irregularities refer to, but are not limited to:

- Any dishonest or fraudulent act.
- Misappropriation of funds, securities, supplies, or other assets.
- Impropriety in the handling or reporting of money or financial transactions.
- Profiteering as a result of insider knowledge of company activities.
- Disclosing confidential and proprietary information to outside parties.
- Disclosing to other person securities activities engaged in or contemplated by the company.
- *Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Company.*
- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment.
- Any similar or related irregularity.

5. OTHER IRREGULARITIES

5.1. Irregularities concerning an employee's moral, ethical, or behavioral conduct should be resolved by departmental management and the Employee Relations Unit of Human Resources rather than the Investigating Unit.

5.2. If there is any question as to whether an action constitutes fraud, contact the head of Internal Audit and/or Legal for guidance.

6. INVESTIGATION

6.1. The Investigating Unit has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. If the investigation substantiates that fraudulent activities have occurred, the Investigating Unit will issue reports to Finance Director and, if appropriate, to the Board of Directors through the Audit Committee.

6.2. Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with legal counsel and senior management, as well as the final decisions on disposition of the case.

6.3. PMPC's fraud response plan should be used in conjunction with this policy. It provide direction and help to those officers and directors who find themselves having to deal with suspected cases of theft, fraud or corruption. It gives a framework for a response and provides information on various aspects of investigation.

6.4. The personnel and/or department who are the primary, secondary and shared responsibility for investigating fraud is summarized in ***Appendix B*** *(Fraud Policy Decision Matrix)* of this policy statement.

7. CONFIDENTIALITY

7.1. The Investigating Unit treats all information received confidentially. Any employee who suspects dishonest or fraudulent activity will notify the Investigating Unit and/or Internal Audit immediately, and should not attempt to personally conduct investigations or interviews/interrogations related to any suspected fraudulent act (see Reporting Procedures section below).

7.2. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the Company from potential civil liability.

8. AUTHORIZATION FOR INVESTIGATING SUSPECTED FRAUD

8.1. Members of the Investigation Unit will have:

- Free and unrestricted access to all Company records and premises, whether owned or rented.
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

9. REPORTING

9.1. Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

9.2. An employee who discovers or suspects fraudulent activity will contact the Investigating Unit immediately. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the Investigations Unit or the Legal Department. No information concerning the status of an investigation will be given out. The proper response to any inquiries is: "I am not at liberty to discuss this matter." Under no circumstances should any reference be made to "the allegation," "the crime," "the fraud," "the forgery," "the misappropriation," or any other specific reference.

9.3. The reporting individual should be informed of the following:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case, facts, suspicions, or allegations with anyone unless specifically asked to do so by the Legal Department or Investigating Unit.

10. TERMINATION

10.1. If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed for approval by the designated representatives from Human Resources and the Legal Department and, if necessary, by outside counsel, before any such action is taken. The Investigating Unit and/or Internal Audit does not have the authority to terminate an employee. The decision to terminate an employee is made by the employee's management. Should the Investigating Unit believe the management decision inappropriate for the facts presented, the facts will be presented to executive-level management for a decision.

11. FRAUD RISK ASSESSMERNT

11.1. Fraud Risk Assessment should be made annually to identify high risk areas so that appropriate mitigating measures are put in place. Appendix C provides an example of Fraud Risk Assessment for revenue recognition. **APPENDIX D** *Fraud Risk Exposure* illustrates the types of frauds an organization might encounter. The listing is not meant to be all- inclusive but to provide a starting point for an organization to identify which areas are vulnerable to fraud.

12. ADMINISTRATION

12.1. The Internal Audit is responsible for the administration, revision, interpretation, and application of this policy. The policy will be reviewed annually and revised as needed. This policy shall be disclosed in the Company's website www.panasonic.com.ph

APPENDIX A: FRAUD POLICY FRAMEWORK

1. EXECUTIVE SUMMARY

- Definition of fraud
- Statement of attitude to fraud
- Code of conduct (relationship to)
- Relationship with entity's other plans
- Roles and accountabilities

2. SUMMARY OF FRAUD CONTROL STRATEGIES

- Appointment of fraud control officer
- External assistance to the fraud control officer
- Fraud control responsibilities
- Fraud risk management (including fraud risk assessment)
- Fraud awareness
- Fraud detection
- Fraud reporting
- Investigation of fraud and other improper conduct
- Internal control review following discovery of fraud
- Fidelity guarantee and criminal conduct insurance
- Internal audit program

3. FRAUD RISK MANAGEMENT

- Regular program for fraud risk assessment
- Ongoing review of fraud control strategies
- Fraud risk assessment
- Implementation of proposed actions

4. PROCEDURES FOR REPORTING FRAUD

- Internal reporting
- Reports by members of staff
- Protection of employees reporting suspected fraud
- External anonymous reporting
- Reports to the police
- Reports to external parties
- Administrative remedies
- Recovery of the proceeds of fraudulent conduct
- Reporting requirements

5. EMPLOYMENT CONDITIONS

- Pre-employment screening
- Annual leave

6. CONFLICT OF INTEREST

- The impact of conflicts of interest
- Register of interests
- Conflict of interest policy

7. PROCEDURES FOR FRAUD INVESTIGATION

- Internal investigations
- External investigative resources
- Documentation of the results of the investigation

8. INTERNAL AUDIT STRATEGY

- Internal audit capability
- Internal audit fraud control function

9. REVIEW OF FRAUD CONTROL ARRANGEMENTS

APPENDIX B: FRAUD POLICY DECISION MATRIX

NOTE: This matrix can be used as a tool to summarize and visualize the responsibilities that have been defined for the organization. This is not a standard for "who" should have "what" responsibilities.

ACTION REQUIRED	INVESTIGATION UNIT	INTERNAL AUDITING	FIN. / ACCTG.	EXEC. MGMT.	LINE MGMT.	RISK MGMT.	PR	EMPLOYEE RELATIONS	LEGAL
1. Controls to Prevent Fraud	S	S	S	P	SR	S	S	S	S
2. Incident Reporting	P	S	S	S	S	S	S	S	S
3. Investigation of Fraud	P	S						S	S
4. Referrals to Law Enforcement	P								S
5. Recovery of Monies Due to Fraud	P								
6. Recommendations to Prevent Fraud	SR	SR	S	S	S	S	S	S	S
7. Internal Controls Reviews		P							
8. Handle Cases of a Sensitive Nature	P	S		S		S		S	S
9. Public/Press Releases	S	S					P		
10. Civil Litigation	S	S							P
11. Corrective Action/Recommendations to Prevent Recurrences	SR	SR		S	SR	S			S
12. Monitor Recoveries	S		P						
13. Proactive Fraud Auditing	S	P							
14. Fraud Education/Training	P	S			S		S		
15. Risk Analysis of Areas of Vulnerability	S	S				P			
16. Case Analysis	P	S							
17. Hotline	P	S							
18. Ethics Line	S	S							P

P (Primary Responsibility) **S (Secondary Responsibility)** **SR (Shared Responsibility)**

APPENDIX C: FRAUD RISK ASSESSMENT

NOTE: This example is for illustrative purposes and focuses solely on potential revenue recognition risks within financial reporting. A full fraud risk assessment would consider fraudulent financial reporting in other areas relevant to the organization, such as accounts subject to estimation, related-party transactions, and inventory accounting. In addition, the risk of misappropriation of assets, corruption, and other misconduct would be assessed in the same manner.

Identified Fraud risks and Schemes (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Existing anti-fraud Controls5)	Controls effectiveness assessment (6)	Residual risks (7)	Fraud risk response(8)
Financial Reporting **Revenue recognition** **Backdating agreements**	Reasonably possible	Material	Sales personnel	Controlled contract administration system	Tested by IA	N/A	Periodic testing by IA
Channel stuffing	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
Holding books open	Reasonably possible	Material	Accounting	Standard monthly close process Reconciliation of invoice register to general ledger Established procedures for shipping, invoicing, and revenue recognition Established process for consolidation	Tested by IA Tested by management Tested by IA Tested by IA	Risk of management override	Testing of late journal entries Cut off testing by IA
Late shipments	Reasonably possible	Significant	Shipping dept.	Integrated shipping system, linked to invoicing and sales register Daily reconciliation of shipping log to invoice register Required management approval of manual invoices	Tested by IA Tested by management Tested by IA	Risk of management override	Cut off testing by IA
Side letters/ agreements	Probable	Material	Sales personnel	Annual training of sales and finance personnel on revenue recognition practices Quarterly signed attestation of sales personnel concerning extra contractual agreements Internal audit confirming with customers that there are no other agreements, written or oral, that would modify the terms of the written agreement	Tested by management Tested by management	Risk of override	Disaggregated analysis of sales, sales returns, and adjustments by salesperson
Inappropriate journal entries	Reasonably possible	Material	Accounting & Finance	Established process for consolidation Established, systematic access controls to the general ledger Standard monthly and quarterly journal entry log maintained. Review process in place for standard entries, and	Tested by IA Tested by IA Tested by management	Risk of override N/A N/A	Data mining of journal entry population by IA for: • Unusual Dr/CR

Identified Fraud risks and Schemes (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Existing anti-fraud Controls5)	Controls effectiveness assessment (6)	Residual risks (7)	Fraud risk response(8)
				nonstandard entries subject to two levels of review			combinations • Late entries to accounts subject to estimation
Roundtrip transactions	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
Manipulation of bill and hold arrangements	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
Early delivery of product	Reasonably possible	Significant	Sales and shipping	Systematic matching of sales order to shipping documentation; exception reports generated.	Tested by management	Adequately mitigated by controls	N/A
Partial shipments	Reasonably possible	Significant	Sales and shipping	Systematic shipping documents manually checked against every shipment. Systematic matching of sales order to shipping documentation; exception reports generated. Customer approval of partial shipment required prior to revenue recognition.	Tested by management	Adequately mitigated by controls	N/A

Risk Assessment Column Explanation:

1. **Identified Fraud Risks and Schemes:** This column should include a full list of the potential fraud risks and schemes that may face the organization. This list will be different for different organizations and should be informed by (a) industry research, (b) interviews of employees and other stakeholders, (c) brainstorming sessions, and (d) activity on the whistleblower hotline.
2. **Likelihood of Occurrence:** To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks so that the organization establishes proper anti-fraud controls for the risks that are deemed most likely. For purposes of the assessment, it should be adequate to evaluate the likelihood of risks as remote, reasonably possible, and probable.

3. **Significance to the Organization:** Quantitative and qualitative factors should be considered when assessing the significance of fraud risks to an organization. For example, certain fraud risks may only pose an immaterial direct financial risk to the organization, but could greatly impact its reputation, and therefore, would be deemed to be a more significant risk to the

organization. For purposes of the assessment, it should be adequate to evaluate the significance of risks as immaterial, significant, and material.

4. **People and/or Department Subject to the Risk:** As fraud risks are identified and assessed, it is important to evaluate which people inside and outside the organization are subject to the risk. This knowledge will assist the organization in tailoring its fraud risk response, including establishing appropriate segregation of duties, proper review and approval chains of authority, and proactive fraud auditing procedures.

5. **Existing Anti-fraud Internal Controls:** Map pre-existing controls to the relevant fraud risks identified. Note that this occurs after fraud risks are identified and assessed for likelihood and significance. By progressing in this order, this framework intends for the organization to assess identified fraud risks on an inherent basis, without consideration of internal controls.

6. **Assessment of Internal Controls Effectiveness:** The organization should have a process in place to evaluate whether the identified controls are operating effectively and mitigating fraud risks as intended. Companies subject to the provisions of The U.S. Sarbanes- Oxley Act of 2002 Section 404 will have a process such as this in place. Organizations not subject to Sarbanes-Oxley should consider what review and monitoring procedures would be appropriate to implement to gain assurance that their internal control structure is operating as intended.

7. **Residual Risks:** After consideration of the internal control structure, it may be determined that certain fraud risks may not be mitigated adequately due to several factors, including (a) properly designed controls are not in place to address certain fraud risks or (b) controls identified are not operating effectively. These residual risks should be evaluated by the organization in the development of the fraud risk response.

8. **Fraud Risk Response:** Residual risks should be evaluated by the organization and fraud risk responses should be designed to address such remaining risk. The fraud risk response could be one or a combination of the following: (a) implementing additional controls, (b) designing proactive fraud auditing techniques, and/or (c) reducing the risk by exiting the activity

APPENDIX D: FRAUD RISK EXPOSURE

The following illustrates the types of frauds an organization might encounter. This listing is not meant to be all- inclusive but to provide a starting point for an organization to identify which areas are vulnerable to fraud. More attention will be needed to identify specific industry, location, and cultural factors that can influence fraudulent behavior. Once identified, the fraud risk assessment framework shown in Appendix C could be used.

1) Intentional manipulation of financial statements can lead to:
- a) Inappropriately reported revenues
  - (1) Fictitious revenues
  - (2) Premature revenue recognition
  - (3) Contract revenue and expense recognition
- b) Inappropriately reported expenses
  - (1) Period recognition of expenses
- c) Inappropriately reflected balance sheet amounts, including reserves
  - (1) Improper asset valuation
    - (a) Inventory
    - (b) Accounts receivable
    - (c) Mergers and acquisitions
    - (d) Capitalization of intangible items
  - (2) Misclassification of assets
  - (3) Inappropriate depreciation methods
  - (4) Concealed liabilities and expenses
    - (a) Omission
    - (b) Sales returns and allowances and warranties
    - (c) Capitalization of expenses
    - (d) Tax liability
- d) Inappropriately improved and/or masked disclosures
  - (1) Liabilities omissions
  - (2) Subsequent events
  - (3) Related-party transactions
  - (4) Accounting changes
  - (5) Management frauds uncovered
  - (6) Backdating transactions
- e) Concealing misappropriation of assets
- f) Concealing unauthorized receipts and expenditures
- g) Concealing unauthorized acquisition, disposition, and use of assets

2) Misappropriation of:
- a) Tangible assets by
  - (1) Cash theft
    - (a) Sales register manipulation
    - (b) Skimming
    - (c) Collection procedures

- (d) Understated sales
- (e) Theft of checks received
- (f) Check for currency substitution
- (g) Lapping accounts
- (h) False entries to sales account
- (i) Inventory padding
- (j) Theft of cash from register
- (k) Deposit lapping
- (l) Deposits in transit

(2) Fraudulent disbursements
- (a) False refunds
- (b) False voids
- (c) Small disbursements
- (d) Check tampering
- (e) Billing schemes
- (f) Personal purchases with company funds
- (g) Returning merchandise for cash

(3) Payroll fraud
- (a) Ghost employees
- (b) Falsified hours and salary
- (c) Commission sales

(4) Expense reimbursement
- (a) Mischaracterized expenses
- (b) Overstated expenses
- (c) Fictitious expenses
- (d) Multiple reimbursements

(5) Loans
- (a) Loans to nonexistent borrowers
- (b) Double pledged collateral
- (c) False application information
- (d) Construction loans

(6) Real estate
- (a) Appraisal value
- (b) Fraudulent appraisal

(7) Wire transfer
- (a) System password compromise
- (b) Forged authorizations
- (c) Unauthorized transfer account
- (d) ATM

(8) Check and credit card fraud
- (a) Counterfeiting checks
- (b) Check theft
- (c) Stop payment orders
- (d) Unauthorized or lost credit cards

(e) Counterfeit credit cards

(9) Insurance fraud

(a) Dividend checks

(b) Settlement checks

(c) Premium

(d) Fictitious payee

(e) Fictitious death claim

(f) Underwriting misrepresentation

(g) Vehicle insurance — staged accidents

(h) Inflated damages

(i) Rental car fraud

(10) Inventory

(a) Misuse of inventory

(b) Theft of inventory

(c) Purchasing and receiving falsification

(d) False shipments

(e) Concealing inventory shrinkage

b) Intangible assets

(1) Theft of intellectual property

(a) Espionage

(b) Loss of information

(c) Spying

(d) Infiltration

(e) Informants

(f) Trash and waste disposal

(g) Surveillance

(2) Customers

(3) Vendors

c) Proprietary business opportunities

3) Corruption including:

a) Bribery and gratuities to

(1) Companies

(2) Private individuals

(3) Public officials

b) Embezzlement

(1) False accounting entries

(2) Unauthorized withdrawals

(3) Unauthorized disbursements

(4) Paying personal expenses from bank funds

(5) Unrecorded cash payments

(6) Theft of physical property

(7) Moving money from dormant accounts

c) Receipt of bribes, kickbacks, and gratuities
- (1) Bid rigging
- (2) Kickbacks
  - (a) Diverted business to vendors
  - (b) Over billing
- (3) Illegal payments
  - (a) Gifts
  - (b) Travel
  - (c) Entertainment
  - (d) Loans
  - (e) Credit card payments for personal items
  - (f) Transfers for other than fair value
  - (g) Favorable treatment
- (4) Conflicts of interest
  - (a) Purchases
  - (b) Sales
  - (c) Business diversion
  - (d) Resourcing
  - (e) Financial disclosure of interest in vendors
  - (f) Ownership interest in suppliers

d) FCPA violations
- (1) Anti-bribery provisions
- (2) Books and records violations
- (3) Internal control weaknesses

e) Money laundering

f) Aiding and abetting fraud by other parties (customers, vendors)

Policy Prepared by:

ANDREI R. TIBI
Internal Auditor

Policy Read and Approved by:

SHINICHI HAYASHI
PMPC President

MASARU TOYOTA
Vice-President PPH Sales / Executive Director

YOSHIYUKI TAKAHASHI
Executive Director

HIROSHI YAMADA
Executive Director

ATTY. MAMERTO MONDRAGON
Corporate Secretary / Compliance Officer

EMILIANO VOLANTE
Audit Committee Chairman / Independent Director

ELIZABETH GILDORE
Audit Committee Member/Independent Director

Date of Signing:

APRIL 5, 2017