



MERALCO
Ang liwanag ng bukas

SUPPLIERS' BUSINESS CONDUCT

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 2 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: Copyright		Date Approved: September 24, 2012	

This document is the intellectual property of MERALCO and should not be copied, reproduced, published or distributed without prior written permission from the Corporate Governance Office of MERALCO.

Prepared by:
Corporate Governance Office

Approved by:
Board of Directors

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 3 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: Letter to Suppliers		Date Approved: September 24, 2012	

Our Valued Suppliers:

MERALCO's (or the Company's) philosophy of "Service Excellence with Integrity" conveys its unwavering commitment to high standards of corporate governance principles and practices. It strives to ensure that every business decision is guided by its commitment to operate with high ethical standards in compliance with all applicable laws, regulations and policies.

Contractors, consultants, vendors and financial institutions (collectively, "Suppliers"), as our business partners, shall also practice high standards of business ethics when they provide goods and services to the Company.



We also believe that the Standards reflected in this document will advance the performance of our companies to our mutual benefit.

We request for your cooperation in complying with Meralco's Suppliers' Business Conduct Guide in order to sustain our partnership with you.

Sincerely,

(Original Signed)

Oscar S. Reyes

President and CEO

Prepared by:
Corporate Governance Office

Approved by:
Board of Directors

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 4 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: Table of Contents		Date Approved: September 24, 2012	

Table of Contents

I.	POLICY STATEMENT	5
II.	PURPOSE AND SCOPE	5
III.	DEFINITION OF TERMS	5
IV.	PRINCIPLES AND STANDARDS (SUMMARY TABLE ¹).....	8
	A. ENVIRONMENT, SAFETY AND HEALTH.....	9
	1. Safety at the Workplace	9
	2. Safety of the Environment.....	9
	3. Emergency Prevention, Preparedness, and Response	10
	B. BUSINESS ETHICS	10
	1. Anti-bribery and Anti-corruption.....	10
	2. Giving Gifts, Meals and Entertainment	11
	3. Conflict of Interest	11
	4. Disclosure of Information	11
	5. Whistleblower Protection and Anonymous Complaints	12
	6. Customer Relations.....	12
	7. Labor and Human Rights.....	12
	8. Legal Compliance	12
	C. USE OF THE COMPANY'S ASSETS	13
	1. Computer and System Security	13
	2. Confidential Information	13
	3. Company Records and Disclosures	14
	4. Retention of Records	14
	5. Endorsements	14
	6. News Media Inquiries	14
	D. PRODUCT AND SERVICE STANDARDS	15
V.	RAISING CONCERNS	15
VI.	COMPLIANCE AND ENFORCEMENT	15
VII.	EFFECTIVITY	17

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 5 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: I. INTRODUCTION		Date Approved: September 24, 2012	

I. POLICY STATEMENT

This Policy is to provide Suppliers as well as the general public with a formal statement of the Company's commitment to conduct its business with uncompromising integrity and professionalism and its adherence to the policies and rules prescribed in the Company's Code of Ethics (COE). Accordingly, Suppliers are necessarily expected to adhere to the Company's fundamental principles of fairness, accountability, integrity and transparency and to commit to high standard of business ethics. Aptly, the Company shall only engage the services of Suppliers who meet the Company's high standards of business ethics.

This Suppliers' Business Conduct or SBC is a Policy that does not confer rights to any vendor nor does it impose any obligations on the Company.

II. PURPOSE AND SCOPE

The SBC is a general guide to acceptable and appropriate conduct and behavior expected from Suppliers of the Company. The term Suppliers is used in its generic sense and shall include suppliers and vendors providing services and goods to the Company, consultants, advisors, financial institutions, and any person or institution who has business transactions with the Company.

The absence of specific guidelines or instructions covering a particular situation does not relieve a Supplier from exercising the highest ethical standards applicable under the circumstances.

III. DEFINITION OF TERMS

For the purpose of this Policy, the following definition of terms shall be used:

1. **AFFILIATED PARTY** – refers to any person, natural or juridical, other than the Company, who has a financial, professional or personal relationship or interest with a director, employee or officer of the Company. These include:
 - a. Relatives of up to the third degree, by consanguinity, affinity or legal adoption, including the legal spouse or a common-law spouse and/or his

Prepared by:
Corporate Governance Office

Approved by:
Board of Directors

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 6 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: III. DEFINITION OF TERMS		Date Approved: September 24, 2012	

relatives of up to third degree, by consanguinity, affinity or legal adoption. For purposes hereof, relatives shall include first cousins (Please see illustration in **Exhibit A: Tracing Affinity and Consanguinity Relations** on page 18);

- b. Corporations or firms other than the Company where a director, officer, employee and/or his relative as defined in “a”, holds a position as director, officer, executive, employee or consultant; or
 - c. Corporations, other than the Company, owned by the directors, officers, employees of the Company, or their relatives, who hold either singly or collectively, more than ten percent (10%) of the subscribed capital or equity of such corporations;
 - d. Partnerships in which a director, officer, employee or a relative as defined in “a” is a partner;
 - e. Co-ownership wherein a director, officer, employee, or his affiliated party is a part owner of the property sold, assigned or leased to the Company;
 - f. Relationship by reason of wedding, baptismal or sponsorship of the employee or of his spouse or children.
2. **COMPANY PREMISES** – means all landholdings and buildings including power stations and sub-stations and all other properties owned or rented by the Company. It also covers the working area occupied by employees assigned on the field including Company vehicles.
 3. **CONFIDENTIAL INFORMATION** – refers to all nonpublic information that might be useful to competitors or harmful to the Company or its customers if disclosed. This includes but is not limited to business plans, products, technical data, specifications, documentation, rules and procedures, contracts, presentations, know-how, product plans, business methods, product functionality, services, data (including customer and employee data), markets, competitive analysis, databases, formats, methodologies, applications, developments, inventions, processes, payment, delivery and inspection procedures, designs, drawings, algorithms, formulas, or

Prepared by:
Corporate Governance Office

Approved by:
Board of Directors

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 7 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: III. DEFINITION OF TERMS		Date Approved: September 24, 2012	

information related to engineering, marketing, or finance and any other information that may be reasonably construed as confidential to the Company.

4. **CONFLICT OF INTEREST** – refers to a situation where financial or business interest, professional, or other personal considerations or interests may influence, jeopardize or compromise, or have the appearance, tendency or propensity of influencing, jeopardizing or compromising, the ability to effectively and impartially or objectively exercise independent judgment in formulating or making decisions and performing duties and responsibilities..
5. **GIFTS OR GRATUITIES** – may be a right or thing of value, like cash or cash equivalent, loan, fee, reward, commission, allowance, employment, travel, accommodation, sponsorship to conferences, seminars or trainings, among others.
6. **MATERIAL INFORMATION** – means information that a reasonable investor would consider important in making an investment decision.
7. **SUPPLIER** – an entity or individual who provides the needed goods or services to the Company, which may be a consultant, vendor, contractor or financial institution. This includes existing and prospective suppliers.
8. **WEAPON** - is a firearm, ammunition, explosive, or any other device or object that can be used to cause physical injuries or death to persons and/or damage to property.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 8 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: IV. PRINCIPLES AND STANDARDS		Date Approved: September 24, 2012	

IV. PRINCIPLES AND STANDARDS (SUMMARY TABLE¹)

A. ENVIRONMENT, SAFETY AND HEALTH 1. Safety at the Workplace through: a. Compliance with Safety and Health Procedures b. Reporting of unsafe conditions in the delivery of service c. Prohibition on illegal drugs, alcohol and weapons 2. Ensure Safety of the Environment by following environmental laws and regulations. 3. Emergency Prevention, Preparedness, and Response plans are in place.	B. BUSINESS ETHICS 1. Strict observance of Anti-bribery and Anti-corruption practices. 2. Prohibition of giving Gifts to Company directors, officers or employees. 3. Avoidance of Conflict of Interest through disclosure of close personal relationships with Company directors, officers or employees. 4. Full compliance to information disclosure on business, financial position and operational performance. 5. Whistleblower Protection and Anonymous Complaints mechanisms are in place. 6. Practice good Customer Relations through Suppliers' professional grooming and conduct. 7. Uphold labor laws and protection of human rights. 8. Compliance to all applicable laws and rules and regulations.	C. USE OF THE COMPANY'S ASSETS 1. Comply with Company's Information Security Policy. 2. Protect the confidential information of the Company. 3. Ensure full, fair, accurate, and timely records, disclosures, and communications to the Company. 4. Adhere to records retention policy of the Company. 5. Shall not use Company logo or trademarks for personal gain. 6. Unauthorized representation of the Company to media or press.
D. PRODUCT AND SERVICE STANDARDS 1. Comply with products and services rules, regulations and statutory requirements; 2. No to collusion or connivance with other suppliers or agents when participating in a bid; 3. Shall not act as an agent or representative of a third party provider of the same products or services; 4. Supply products that are certified of good quality; 5. Possess the necessary capabilities, equipment and suitable place of business; 6. No subcontracting or outsourcing unless with prior written consent from the Company; 7. Maintain the highest standards of integrity and quality of work at all times.		

¹ Details are in the succeeding pages.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 9 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: IV. PRINCIPLES AND STANDARDS		Date Approved: September 24, 2012	

A. ENVIRONMENT, SAFETY AND HEALTH

1. Safety at the Workplace

The Company strives to provide each employee, officer and other stakeholders with a safe and healthy environment. As such, the Suppliers are expected to perform their company related-work in a safe manner, free from the influence of alcohol, illegal drugs or controlled substance and to help and encourage others to work safely, and always put safety first.

Towards this end, all Suppliers shall at all times ensure:

Compliance with the all applicable environmental and workplace safety and health rules and regulations, by:

- a. Immediately reporting to the Company business contact all accidents, occupational injuries and illnesses, and any unsafe equipment, practices or conditions that it cannot immediately correct.
- b. Being mentally and physically fit to perform the services expected of them; and
- c. Non-toleration of any kind of violence including threatening behavior and prohibiting the bringing in, possessing, storing or using of any type of weapon or prohibited drugs or controlled substances within the Company premises or Company assigned work areas.

The Company retains the right to review the Supplier's safety procedures and specify additional requirements in its contract with them, if necessary.

2. Safety of the Environment

Suppliers are committed to conduct its business in an environmentally responsible manner and comply fully with all the applicable environmental laws and regulations.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 10 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: IV. PRINCIPLES AND STANDARDS		Date Approved: September 24, 2012	

3. Emergency Prevention, Preparedness, and Response

Whenever applicable, Suppliers shall anticipate, identify, and assess emergency situations and events and minimize their impact by implementing emergency plans and response procedures, including emergency reporting, worker notification and evacuation procedures, worker training and drills, appropriate first-aid supplies, appropriate fire detection and suppression equipment, adequate exit facilities, and recovery plans.

Suppliers that support the Company's real-time operation and financial functions shall have its Business Continuity plans in place and regularly tested to sustain the supply and/or delivery of its services despite the occurrence of an emergency, crisis situation, natural disaster or security related event. Suppliers may be asked to provide the Company with copies of their plans, exercise and training records.

B. BUSINESS ETHICS

1. Anti-bribery and Anti-corruption

Corruption, extortion, and embezzlement, in any form or manner, are strictly prohibited. Suppliers shall comply at all times with all applicable anti-bribery and anti-corruption laws. Suppliers shall not offer, accept, promise, pay, permit or authorize bribes and kickbacks, which include giving gifts to the Company's Directors, Officers or Employees or other means to obtain an undue or improper advantage.

Suppliers shall ensure that their business records including all requests for payments, fully and accurately reflect transactions, expenditures and/or services performed.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 11 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: IV. PRINCIPLES AND STANDARDS		Date Approved: September 24, 2012	

2. Giving Gifts

Suppliers are prohibited from giving gifts to Directors, Officers, and Employees of the Company.

Tokens like corporate giveaways as customary business courtesies may be allowed on exception cases but should be governed by the Company's Policy on Solicitation and Acceptance of Gifts (Gift Policy). Gifts of cash or cash equivalents, such as gift cards, are never allowed.

Immediate disclosure to Meralco's Corporate Governance Office is required in case the Supplier insists on providing gifts of any value to the Company's directors, officers and employees.

Suppliers shall seek clearance from their business contacts in the Company or the Meralco's Corporate Governance Office, prior to undertaking actions that are covered by or have implications on the provisions of Gift Policy in order to avoid violations.

3. Conflict of Interest

It has always been and continues to be the intent of the Company that its Suppliers maintain the highest ethical standards in the conduct of its business. The Company expects its Suppliers to conduct its business with the highest degree of integrity, fairness and transparency, in accordance with all applicable rules and regulations and in a manner that excludes consideration of personal advantage. Suppliers are required to declare any material personal interest which may affect or be seen to affect the work they are contracted to perform. Strict adherence to this Policy will protect the Company and Suppliers from criticism, litigation or embarrassment that might result from alleged or real conflicts of interest or unethical practices

4. Disclosure of Information

Suppliers shall accurately record and disclose information regarding their business activities, structure, financial situation, and performance in accordance with applicable laws and regulations and prevailing industry practices.

Prepared by:
Corporate Governance Office

Approved by:
Board of Directors

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 12 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: IV. PRINCIPLES AND STANDARDS		Date Approved: September 24, 2012	

5. Whistleblower Protection and Anonymous Complaints

Suppliers shall create appropriate program/s that will protect and ensure the confidentiality of whistleblowers and prevent retaliation against those who participate in such programs. Suppliers shall provide an anonymous complaint mechanism to report workplace grievances in accordance with local laws and regulations.

6. Customer Relations

The Company values the satisfaction and loyalty of its customers. Suppliers charged with servicing these customers shall ensure that services rendered are delivered timely, adequately and with the highest degree of quality. Proper decorum and good customer relations are to be observed at all times.

7. Labor and Human Rights

Suppliers shall provide equal opportunity in all aspects of employment and shall not tolerate any illegal discrimination or harassment based on color, race, religion, nationality, origin, age, gender, marital status, sexual orientation, disability, or political affiliation.

Suppliers shall respect the personal dignity, privacy and rights of each individual by prohibiting behavior including gestures, language and physical contact that is sexual, coercive, threatening, abusive or exploitative and shall ensure equality in the workplace with no discrimination.

Suppliers shall not engage the services of children or employ workers who are under the allowed legal age of employment in the pertinent country or local jurisdiction where they are located.

8. Legal Compliance

All Suppliers shall respect and comply with all applicable laws, rules, regulations and local ordinances, including those relating to taxation, employment, human rights, the environment, health and safety where they operate.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 13 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: IV. PRINCIPLES AND STANDARDS		Date Approved: September 24, 2012	

C. USE OF THE COMPANY'S ASSETS

The Company's assets such as computers, telephones and cell phones, fax machines, copy machines, conference rooms, vehicles, construction equipment, tools, and similar assets, which are within the disposal of the Supplier, shall be used solely and exclusively for the Company's business.

1. Computer and System Security

Suppliers who have access to the Company's information systems are fully responsible and accountable for the security of those systems and shall strictly comply with the Company's information security policies and standards. (Please refer to **Exhibit C for the Information Security Policies for External Parties** on page 20).

2. Confidential Information

Suppliers shall not be given access to proprietary and/or confidential information of the Company unless authorized under a non-disclosure agreement, as such Suppliers are prohibited from copying, sharing, disseminating or using these information to discredit the Company or to gain personal advantage or benefit. For this reason, Suppliers with authorized access shall:

- a. Maintain the confidentiality of information entrusted to them and on the Company's customers, except when disclosure is properly authorized or legally mandated. This includes any information about a specific customer such as but not limited to the customer's name, address, Social Security number, phone numbers, contact names, and billing data.
- b. Not share confidential information with Affiliates or other related parties without appropriate approval from the Company.
- c. Not disclose non-public Material Information acquired while working with the Company that can be used in making investment decisions concerning the Company's securities. The Company's Insider Trading (Black Out) Policy prohibits trading while in possession of material nonpublic information and prohibits sharing this information with others to enable them to trade.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 14 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: IV. PRINCIPLES AND STANDARDS		Date Approved: September 24, 2012	

Supplier's commitment on the treatment of the Company's confidential information shall be binding even after the termination or expiration of Suppliers' engagement with the Company.

3. Company Records and Disclosures

Accurate records and disclosures are critical to the Company in meeting its legal, financial, regulatory, and management obligations. Suppliers shall ensure that all records, disclosures, and communications to the Company are full, fair, accurate, timely, and understandable.

Suppliers shall not hide, alter, falsify, or disguise the true nature of any transaction, nor forge endorsements, approvals, or authorizing signatures for any payment. If a record or disclosure is known to be misleading or false, this shall not be submitted, encoded, processed, or approved and shall be reported immediately to its business contact in the Company.

4. Retention of Records

Suppliers shall implement document retention periods as may be reasonably prescribed by the Company.

5. Endorsements

Suppliers shall not use the Company's name or trademarks in advertising, publicity, articles, catalogs, testimonials or product endorsements unless duly authorized in writing by the Company.

6. News Media Inquiries

Suppliers shall not make any representation or statement to the media or to anyone on behalf of the Company unless they are expressly authorized to do so by the Company. All inquiries from media or anybody shall be referred to Corporate Communication or Corporate Marketing Office of the Company.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 15 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: IV. PRINCIPLES AND STANDARDS		Date Approved: September 24, 2012	

D. PRODUCT AND SERVICE STANDARDS

Suppliers that seek to do business with the Company shall demonstrate the ability to add value, and provide high-quality goods and services that are competitively priced, reliable, and aligned with its superior level of service.

Suppliers shall abide with the following:

1. Comply with all rules, regulations and statutory requirements relating to the provision of the products/services to the Company;
2. Not act in collusion or connivance with other suppliers or agents when participating in a bid;
3. Supply only the products that are certified to be of good quality;
4. Possess the necessary capabilities, equipment and suitable place of business to perform its obligations;
5. Not contract out, subcontract or outsource any portion of the products or services except with prior written consent of the Company;
6. Maintain the highest standards of integrity and quality of work at all times.
7. Supports fair competition based on quality, service and price.

V. RAISING CONCERNS

The standards of conduct described in this Policy are critical for the success of the Company's business relationship with its Suppliers. Suppliers are encouraged to report to the Company through its Corporate Governance Office any violations, breach or questionable activities that may prejudice the Company.

VI. COMPLIANCE AND ENFORCEMENT

- A. **Suppliers** shall be responsible and accountable for providing accurate, complete and updated information required in the SBCC Form (Please see **Exhibit B**, page 20) and shall comply with the relevant disclosure requirements prescribed by the Company.

Prepared by:
Corporate Governance Office

Approved by:
Board of Directors

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 16 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: VI. COMPLIANCE AND ENFORCEMENT		Date Approved: September 24, 2012	

- B. The **Nomination and Governance Committee (Nom & Gov)** shall oversee compliance of this Policy through the **Corporate Governance Office (CGO)**. CGO shall oversee compliance of the different organizations, review and recommend amendment to this Policy whenever necessary.
- C. **Procurement Office and Treasury Operations (for Financial Institutions)** shall be responsible for:
 - a. Informing Suppliers of the Company of the SBC and ensure their commitment by facilitating the signing of the appropriate commitment form;
 - b. Administration of the Suppliers' Conflict of Interest Disclosure Form;
 - c. Reviewing and validating the accuracy of the disclosed information by the Supplier; and
 - d. Random checking of Suppliers' compliance to SBC.
- D. **Materials Process Management** shall develop the implementing rules and regulations of this Policy to properly guide the compliance of Suppliers and concerned offices of the Company.
- E. **Corporate Audits** shall conduct random review of the compliance of concerned organizations to this Policy; recommend appropriate sanctions to those found violating it. It also recommends improvements in risk mitigation and internal control procedures to this Policy.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 17 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: VII. EFFECTIVITY		Date Approved: September 24, 2012	

VII. EFFECTIVITY

This Company Policy on Suppliers Business Conduct was approved by the Board of Directors on **September 24, 2012**.

It shall take effect on **October 1, 2012**.

All existing policies, systems, practices, and related implementing guidelines concerning the same matters covered by this Policy are deemed superseded by this Policy. In the event of any inconsistency between the policy and guidelines contained in this Policy and the terms of other existing policies, systems, practices, and related implementing guidelines, this Policy shall prevail.

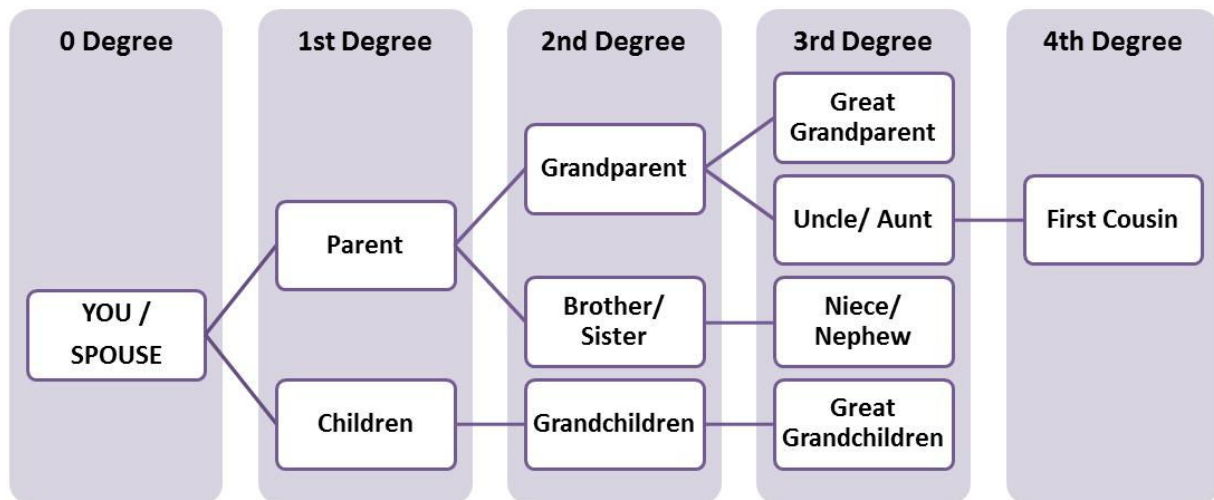
Signed by:

(Original Signed)
OSCAR S. REYES
President and CEO

(Original Signed)
MANUEL V. PANGILINAN
Chairman of the Board

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 18 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: EXHIBIT A		Date Approved: September 24, 2012	

Exhibit A: Tracing Affinity and Consanguinity Relations



Notes:

1. A spouse (legal or common law) is related by marriage (affinity) to his partner's relatives in the same way that he/she is related to them by blood (consanguinity).
2. Half-blood relationship is the same as a full-blood relationship.
3. Step relationship is the same as a blood relationship.
4. For the purpose of this Policy, relationship through adoption shall be considered as part of consanguinity relation.

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 19 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: EXHIBIT B		Date Approved: September 24, 2012	

Exhibit B: Suppliers' Business Conduct Commitment (SBCC) Form.



**Statement of Commitment to
MERALCO'S SUPPLIERS BUSINESS CONDUCT**

1. I understand that MERALCO (or the Company) is committed to uphold the fundamental corporate governance principles of fairness, accountability, integrity and transparency.
2. I have fully read and understood the provisions of the attached MERALCO'S Suppliers Business Conduct (SBC).
3. I therefore commit to:
 - a. Personally exhibit and promote the highest standards of honest and ethical conduct, including personal compliance with the SBC provisions.
 - b. Ensure that all my employees are fully aware of this code of conduct and are also committed to comply with it.
 - c. Promptly report to my MERALCO business contact or partner or the Corporate Governance Office any non-compliance to the COE, laws, rules, regulations, or Company policies and procedures.
4. I understand that my non-compliance with the SBC shall result in appropriate sanctions and disciplinary actions by the Company.
5. I am authorized by my company to sign and accept this document on its behalf.

Signed on this ____ day of _____, 20__.

Supplier: _____

Address: _____

Representative: _____

Printed Name and Signature

Date Signed: _____

Position Title: _____

Prepared by:
Corporate Governance Office

Approved by:
Board of Directors

	POLICY Suppliers Business Conduct	PM-CGO-2011-08 Rev. Code: 0	Page 20 of 20
Business Process: Corporate Governance Process		Date Prepared: March 2, 2012	
Section: EXHIBIT C		Date Approved: September 24, 2012	

Exhibit C: Information Security Policies for External Parties



INFORMATION SECURITY POLICIES FOR EXTERNAL PARTIES

Prepared by:
Corporate Governance Office

Approved by:
Board of Directors



INFORMATION SECURITY POLICIES FOR EXTERNAL PARTIES



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page I-2

Section: User's Guide

Effectivity Date: March 1, 2012

Subject: Table of Contents

Document Classification: Public

Table of Contents

Section	Subject	Title	Page Number
I	USER'S GUIDE		
	01	Table of Contents	I-2
	02	Purpose and Scope	I-3
	03	Revision History	I-4
	04	Approval Page	I-5
II	INTRODUCTION		II-1
	A	Definition of Terms	II-2
III	APPLICABLE POLICIES FOR EXTERNAL PARTIES		III-1
	2. ORGANIZATIONAL SECURITY		III-2
	2	Policy Statement	III-3
	2.2	Security in External Party Access	III-4
	3. ASSET MANAGEMENT		III-6
	3	Policy Statement	III-7
	3.3	Information Asset Handling	III-8
	5. PHYSICAL AND ENVIRONMENTAL SECURITY		III-9
	5	Policy Statement	III-10
	5.1	Physical Access Security	III-11
	6. COMMUNICATIONS AND OPERATIONS MANAGEMENT		III-12
	6	Policy Statement	III-13
	6.2	Third Party Service Delivery Management	III-14
	7. ACCESS CONTROL		III-15
	7	Policy Statement	III-16
	7.1	Access Control Policy	III-17

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page I-3

Section: User's Guide

Effectivity Date: March 1, 2012

Subject: Purpose and Scope

Document Classification: Public

**MANILA ELECTRIC COMPANY
INFORMATION SECURITY POLICY MANUAL FOR EXTERNAL PARTIES**

Manila Electric Company (MERALCO) owns a lot of information assets critical to its business. These information assets and how these assets are managed (stored, handled, classified, updated, protected and accessed) are advantages that Meralco has over its competitors. Thus, a corporate Information Security is in place to serve as guide for the company in protecting its information.

With dealings to a growing network of external parties (vendors, outsourcers, potential business partners, etc), Meralco aims to protect its information asset while engaging business with these external parties as well.

As such, the policies specified in this document are extracted from the company's Information Security policy. This Information Security Policy Manual for external parties shall be used to help them understand Meralco's Information Security Policies at a glance.

This manual contains an extract from the Corporate Information Security policies which are deemed applicable to external parties, namely:

SECTION 2: Organizational Security
SECTION 3: Asset Management
SECTION 5: Physical and Environmental Security
SECTION 6: Communications and Operations Management
SECTION 7: Access Control

This manual as of March 1, 2012 is the first version of the Information Security Policy for External Parties.

MARTHYN S. CUAN
Chief Information Officer

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page I-4

Section: User's Guide

Effectivity Date: March 1, 2012

Subject: Revision History

Document Classification: Public

Revision History

Section	Subject	Approval Date	Reason for Change	No. of Pages

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page I-5

Section: User's Guide

Effectivity Date: March 1, 2012

Subject: Approval Sheet

Document Classification: Public

Approval Sheet

We have reviewed the contents of this document described specifically as Information Security Manual for External Parties, and thereby approve its implementation effective March 1, 2012.

Reviewed by :

(Original Signed)

Juan Carlo S. Casem

Head, ICT Planning

(Original Signed)

Elizabeth T. Cruz

Head, Information Systems

(Original Signed)

Bernardo B. Imperial

Head, Information Technology

(Original Signed)

Antolin R. Habaña

Head, Telecommunications

Approved By :

(Original Signed)

Marthyn S. Cuan

Chief Information Officer

Prepared by:

ICT Planning- Information Security

Approved by:

Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page II-1

Section: Introduction

Effectivity Date: March 1, 2012

Subject: Title

Document Classification: Public



INTRODUCTION

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Page II-2

Section: Introduction

Effectivity Date: March 1, 2012

Subject: Definition of Terms

Document Classification: Public

A. Definition of Terms

- A.1. ACCESS CONTROL.** A method for limiting or permitting accesses to a resource or physical premises to authorized entities. Access control may be an administrative, physical, or logical/technical control.
- A.2. ACCESS PRIVILEGES.** The permission granted to: (1) physically enter restricted areas such as communication rooms, data center, etc; (2) use information systems to create, delete, read or modify data or information, according to defined rules for access.
- A.3. CONFIDENTIAL INFORMATION.** Information that must be made available or disclosed only to authorized individuals, entities or processes covered by a Non- Disclosure Agreement (NDA).
- A.4. CONTROLS.** Technological devices or measures that may be used to reduce threats and vulnerabilities, and protect information assets through detection, prevention, and recovery.
- A.5. EXTERNAL PARTY.** Refers to entities or individuals not under the employ nor in the active payroll of the company (i.e. consultants, contractuals, visitors, etc)
- A.6. ICT SYSTEMS/ICT RELATED SYSTEMS (Information and Communication Technology Systems).** Refers to a set-up that includes any communication device encompassing radio, computer and network hardware, satellite systems, etc., as well as the software or applications associated with these devices.
- A.7. INFORMATION ASSET.** A definable piece of information, stored in any manner. Examples of information assets are:
- Information systems files, databases, programs and other system objects needed to execute the application system
 - All supplies used by the application system (e.g. computer forms, bills, purchase order forms, call orders, etc.)
 - Products of processed data extracted from application systems (e.g. reports, statistics, summaries, etc.)
 - Network infrastructure
 - Computer Hardware and Software

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page II-3

Section: Introduction

Effectivity Date: March 1, 2012

Subject: Definition of Terms

Document Classification: Public

- Other documentation such as evaluation reports, special studies, etc.
- Copyrighted and/or proprietary materials

A.8. INFORMATION SECURITY. The preservation or protection of the **confidentiality, integrity and availability of the information assets** against threats like unauthorized access and disclosure, unauthorized modification and damage, theft and denial of service, in order to ensure business continuity, minimize business damage and maximize return on investments.

A.9. NETWORK. Pertains to the data/voice/video communication infrastructure component of the ICT system.

A.10. NON-DISCLOSURE AGREEMENT. A legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by third parties. It is a contract through which the parties agree not to disclose information covered by the agreement.

A.11. POLICY. The overall intention and direction as formally expressed by the management.

A.12. PROCEDURE. A series of tasks that make-up the chronological sequence and established way of performing the work to be accomplished.

A.13. USER. A person, organization entity, or automated process that accesses a system, whether authorized to do so or not.

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-1

Section: Applicable Policies for External Parties

Effectivity Date: March 1, 2012

Subject: Title

Document Classification: Public



**APPLICABLE POLICIES
FOR EXTERNAL PARTIES**

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-2

Section: Organizational Security

Effectivity Date: March 1, 2012

Subject: Title

Document Classification: Public



ORGANIZATIONAL SECURITY

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Page III-3

Section: Applicable Policies for External Parties

Effectivity Date: March 1, 2012

Subject: Policy

Document Classification: Public

2. Organizational Security

"A MANAGEMENT FRAMEWORK THAT DEFINES THE ROLES AND RESPONSIBILITIES, PROCESSES, AND METHODOLOGIES SHALL BE ESTABLISHED TO INITIATE, CONTROL AND MANAGE THE IMPLEMENTATION OF INFORMATION SECURITY ACROSS THE COMPANY, INCLUDING CORRELATION WITH EXTERNAL PARTIES."

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Page III-4

Section: Organizational Security

Effectivity Date: March 1, 2012

Subject: Security of External Party Access

Document Classification: Public

2.2 Security of External Party Access

2.2.1 Access Privileges for External Party

Access privileges shall be granted only to those with explicit authorization in writing from the Management and/or the Information Asset Custodian that specifies the access privileges and the duration of the access.

2.2.1.2 System Access

External parties with a legitimate business need to access ICT-related systems shall require a written authorization from the concerned office head or BRU Head. A Meralco employee shall oversee the system access of the temporarily authorized external party.

2.2.1.2 Physical Access.

External parties with a legitimate business need to access restricted company areas shall require a written authorization from the concerned office head or BRU Head, or Security Office. A Meralco employee shall oversee a temporarily authorized external party during the latter's access to the restricted company area.

2.2.2 External Party Agreements

All agreements that involve use of information assets by an External Party shall have information security provisions. This shall include but shall not be limited to the terms and conditions on the use of information assets and the information security responsibilities of the External Party.

2.2.3 External Party Requests for Information

Any external party who wishes to have access to information about the Company (not confidential and not for company-use information), shall make a written request directly to the Approving Authority.

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-5

Section: Organizational Security

Effectivity Date: March 1, 2012

Subject: Security of External Party Access

Document Classification: Public

2.2.4 Disclosure of Company-Use or Confidential Information to External Party

All confidential or company-use information shall only be disclosed to an External Party when expressly authorized in writing by the Management and/or Information Asset Custodian or Approving Authority. Disclosure shall be preceded by a written non-disclosure agreement between parties, which shall include the purpose of disclosure and validity date of the agreement and all agreements that may be required by policies and guidelines that may be adopted by the company.

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-6

Section: Asset Management

Effectivity Date: March 1, 2012

Subject: Title

Document Classification: Public



ASSET MANAGEMENT

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-7

Section: Asset Management

Effectivity Date: March 1, 2012

Subject: Policy Statement

Document Classification: Public

3. Asset Management

"INFORMATION ASSETS SHALL HAVE DESIGNATED CUSTODIANS AND SHALL BE APPROPRIATELY CLASSIFIED ACCORDING TO THEIR SENSITIVITY AND CRITICALITY TO THE BUSINESS OF THE COMPANY TO ENSURE THAT THE INFORMATION ASSETS RECEIVE AN APPROPRIATE LEVEL OF PROTECTION."

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Page III-8

Section: Asset Management

Effectivity Date: March 1, 2012

Subject: Information Asset Handling

Document Classification: Public

3.3 Information Asset Handling

3.3.1 Information Asset Handling

All authorized users shall observe proper usage, reproduction, storage, transport, disclosure, disposal and other acts in accordance with the applicable guidelines, procedures and policies.

3.3.1.4 Disclosure of Information Assets

Confidential and company-use information shall be made known to users who have a legitimate business need upon authorization of the Information Asset Custodian. Such authorized users shall maintain the confidentiality of all obtained information at all times

3.3.3 Handling of Information Assets from External Sources

All information assets from external sources shall be subject to the handling requirements specified by its source company.

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-9

Section: Physical and Environmental

Effectivity Date: March 1, 2012

Subject: Title

Document Classification: Public



PHYSICAL AND ENVIRONMENTAL SECURITY

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Section III-10

Section: Physical and Environmental Security

Effectivity Date: March 1, 2012

Subject: Policy Statement

Document Classification: Public

5. Physical and Environmental Security

"INFORMATION ASSETS SHALL BE PROVIDED WITH SUITABLE PHYSICAL PROTECTION TO PREVENT UNAUTHORIZED ACCESS, COMPROMISE, DAMAGE, OR THEFT AND INTERRUPTION TO BUSINESS ACTIVITIES. "

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Page III-11

Section: Physical and Environmental Security

Effectivity Date: March 1, 2012

Subject: General Physical Security Controls

Document Classification: Public

5.1 Physical Access Security

5.1.1 Physical Access Control for Areas Containing Company-Use or Confidential Information Assets

Access to every office, computer room, communication room and work area containing company-use or confidential information assets shall be physically restricted as determined by the BRU Head responsible for the area taking into consideration Information Security requirements.

Individuals with a legitimate business who need to access restricted company areas shall require a written authorization from the concerned office head or BRU Head or Security Office. If necessary, an authorized individual shall oversee temporarily authorized personnel.

Proper identification and/or access pass should be provided and worn at all times while within these premises.

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-12

Section: Communications and Operations Mgmt.

Effectivity Date: March 1, 2012

Subject: Title

Document Classification: Public



COMMUNICATIONS AND OPERATIONS MANAGEMENT

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-13

Section: Communications and Operations Mgmt.

Effectivity Date: March 1, 2012

Subject: Policy Statement

Document Classification: Public

6. Communications and Operations Management

"RESPONSIBILITIES, STANDARDS, GUIDELINES, AND PROCEDURES FOR THE MANAGEMENT AND OPERATION OF INFORMATION PROCESSING FACILITIES SHALL BE ESTABLISHED TO PROTECT INFORMATION ASSETS THROUGHOUT THEIR PROCESSING CYCLE."

Prepared by:
Enterprise Architecture Office- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Page III-14

Section: Communications and Operations Mgmt.

Effectivity Date: March 1, 2012

Subject: Third Party Service Delivery Management

Document Classification: Public

6.2 Third Party Service Delivery Management

6.2.1 Monitoring and Review of Third Party Services

The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

The concerned BRU shall ensure that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



**INFORMATION SECURITY
MANAGEMENT**

Rev. Code 0

Page III-15

Section: Communications and Operations Mgmt.

Effectivity Date: March 1, 2012

Subject: Acceptable Use of Information Assets

Document Classification: Public



ACCESS CONTROL

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Page

Section: Access Control

Effectivity Date: March 1, 2012

Subject: Policy Statement

Document Classification: Public

7. Access Control

"ACCESS AND USE OF INFORMATION ASSETS SHALL BE CONTROLLED, AUTHORIZED, MONITORED AND RESTRICTED TO PERSONS WITH A LEGITIMATE BUSINESS NEED."

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer



INFORMATION SECURITY MANAGEMENT

Rev. Code 0

Page 7-3

Section: Access Control

Effectivity Date: March 1, 2012

Subject: Access Control Policy

Document Classification: Public

7.1 Access Control Policy

7.1.1 Access to Information Assets

Access to information assets is a privilege that shall be granted only to those whose responsibilities require such a need. This privilege may be revoked anytime when there is a just cause for the Company to do so in order to ensure the security, of the information asset.

7.1.2 Access Control for Information Assets

Access to information assets shall at all times be controlled. The Information Asset Custodian shall be responsible for implementing controls and maintaining a list that reflects the appropriate access privileges to information assets. The access privilege shall be regularly reviewed by the Information Asset Custodian

Prepared by:
ICT Planning- Information Security

Approved by:
Chief Information Officer