



Marico's Code of Conduct (CoC)

Code Of Conduct

Originally Adopted by the Board of Directors on October 26, 2010

First Amendment to the Code of Conduct adopted by the Board of Directors on January 31, 2014

This Code of Conduct will be known as Marico's Unified Code of Conduct. (Hereinafter to be referred to as "the Code / this Code")

This Code is applicable to all Members.

For the purpose of this Code, the following terms will have the meaning assigned to it as hereunder, unless the context otherwise requires

1. "Member" means
 - i) a director (executive or non-executive) and an employee whether part-time or full-time, fixed term, permanent trainee of Marico Limited, its subsidiaries and all corporates in which Marico Limited or its subsidiaries have management control; or
 - ii) an individual who is a temporary staff, intern, secondee, an apprentice; or
 - iii) a third party or parties who represent the Company or act on behalf of the Company ;
2. "Audit Committee" means the Committee of the Company constituted by the Board of Directors of the Company.
3. "Chairman" means Chairman of Marico Limited.
4. "Corporate Governance Committee" means the Committee of the Company constituted by the Board of Directors of the Company.
5. "Company" shall mean Marico Limited and its subsidiary companies
6. "Improper Activities" including but not limited to :
 - i) Questionable accounting, internal accounting controls or auditing matters
 - ii) Disclosures in documents filed by the Company with statutory authorities and other public disclosures made by the Company that may not be complete or accurate
 - iii) Fraudulent financial reporting
 - iv) Violation of any policies of the Company
 - v) Violation of laws applicable to the Company
 - vi) Fraud against company's shareholders
 - vii) Forgery or alteration of any documents
 - viii) Misappropriation or misuse of Company resources, such as funds, supplies or other assets;
 - ix) Pursuits of a benefit or advantage in violation of conflict of interest policy of the Company state herein above
 - x) Unauthorized alteration or manipulation of computer files
 - xi) Disclosure of confidential information without any authorization
 - xii) Any other act or omission which involves gross misconduct and / or violation of any provision of this Code

Guiding Principles

The underlying philosophy of this code is to conduct our business in an ethical manner as well as create a work environment that is conducive to members and associates alike, based on our values and beliefs.

To help us meet this commitment, the code defines what we expect of our members and associates. This code of conduct sets out guidelines for each individual in the group to follow.

The Code does not cover every eventuality or situation and the laws in each country also differ. Where you encounter situations not covered by the Code, always reflect on the spirit of the Code and values of Marico to make a decision based on common sense and good judgment. In case of any doubts, please consult with your supervisor and / or your HR Representative

The provisions of the Code shall be in addition to and not in derogation of the provisions of any other law for the time being in force. Where differences exist as the result of local customs, norms, laws or regulations, you may apply either the code or local requirements - whichever is more stringent and sets highest standards of recommended behaviour.

If compliance with the Code conflicts with any local laws and / or practices, please notify this immediately to the Code of Conduct Committee (CCC). The Code establishes principles for business conduct applicable throughout the group, regardless of location. The organization will support and stand by all decisions taken by Members in the spirit of trust and membership.

i) Conflict of Interest	8
ii) Receiving and giving gifts and entertainment	9
iii) Bribery	10
iv) Working with Associates	10
v) Compliance with laws of the Land	11

i) Accurate and complete data, records, reporting and accounting	14
ii) Usage of Company Assets	15
iii) Electronic Usage	15
iv) Insider trading	15
v) Confidentiality	16
vi) Information Security	16

i) Equal Opportunity Workplace	18
ii) Harassment free workplace	18
iii) Abuse – substance / Alcohol	19
iv) Abuse of Position / Designation - Bullying	19
v) Racial and religious vilification	19
vi) Respecting Privacy & Confidentiality Of Members	19
vii) Dress Code	20
Viii) Internet Social media Policy	20

YOUR RESPONSIBILITIES

BUSINESS
INTEGRITY

COMPANY ASSETS AND
FINANCIAL INTEGRITY

WORKPLACE
INTEGRITY

1. Various contact points	22
2. Administration and Governance of the Code	22
3. Role and Functions of HR and IT Committee	23
4. Role and functions of Whistle Blower Committee	23
5. Role and functions of Prevention of Sexual Harassment Committee (PoSH)	23
6. Broad Principles of Code of Conduct Committee (CCC)	24
7. Reporting of Grievances & Redressal	24
8. Responsibilities of CCC	24
9. Modifications	25
10. Meetings of CCC	25
11. Quorum of CCC Meeting	26
12. Maintenance of case files, records and reports	26
13. Anonymity and Confidentiality	26
14. Investigations	27
15. Detailed description of the Investigation Process	27
16. Decision of CCC	28
17. Disciplinary Actions	28

Annexure I	
Policy for Prevention of Sexual harassment at work place	30
Annexure II	
Members of Code of Conduct Committee	36
Annexure III	
Marico's Code of Business Ethics	38
Annexure IV	
Marico Information Security Policy 2013	40
Annexure V	
Marico Employees (Dealing In Securities & Prevention Of Insider Trading) Rules, 2012	68

**GREIVENCE
REDRESSAL
MECHANISM**

ANNEXURES

**ACKNOWLEDGMENT
/ CONSENT FORM**



Marico's Code of Conduct (CoC)



YOUR RESPONSIBILITIES **BUSINESS INTEGRITY**



ALL IS NOT FAIR
... in the war at work!





BUSINESS INTEGRITY

i. Conflict of Interest

You shall act in the best interest of the Company at all times.

Conflicts of interest situations arise when Member's personal, social, financial or political activity conflicts with Member's objectivity at work or conflicts directly or indirectly with the interests of the Company.

Members shall not directly or indirectly:

- a) Compete against the Company
- b) Use their position or influence to secure an improper benefit for themselves or others.
- c) Use Company information, assets or resources for their personal gain or the improper benefit of others
- d) Take advantage of inside information or their position with the Company.

You shall not directly or indirectly:

- accept any simultaneous employment with suppliers, customers, competitors or engage in any activity that enhances or supports a competitor's position as this is a direct conflict of interest. Additionally, you shall disclose to immediate supervisor and your HR representative of any interest that you may have with the business of the Company.
- accept position as a Board Member in any other company without obtaining prior written approval from the Chairman. (This does not apply to the non-Executive members of the Board of Directors of the Company)
- invest in a manner that may adversely affect your decision to make objective decisions on behalf of the Company. You shall immediately declare to your supervisor and HR representative about any "substantial interest" you may have or already have in any competitors, supplier or customer (substantial interest may be commonly understood as anything more than 1% of the stocks of a public company). However, if you have a discretionary authority in dealing with that company, any investment would be considered a conflict of interest.
- exploit, for personal gain, any opportunities that are discovered through the use of the Company's property, information or position, unless the opportunity is disclosed fully in writing to the Board of Directors and the Board declines to pursue such opportunities for the Company.

Further, you shall promptly disclose to your supervisor and HR representative any professional interaction with close relatives who could be prospective member, business associates, vendors, competitors where a situation of conflict of interest can arise. (Close Relative means spouse, partner, fiancé/ fiancée, parent, step-parent, child, step-child, sibling, step-sibling, nephew, niece, aunt, uncle, grandparent, grandchild and in-law).

Co-Member relationships

If you are or become involved in relationship with a co-Member then you shall discuss this issue with your immediate Supervisor and HR representative. Such issue shall be handled sensitively but it will be necessary to make changes to your working environment or reporting structure, including transferring one or both Members to avoid any conflict. Care should be taken proactively by the concerned Members that their behaviour towards each other does not cause discomfort to Members around.

When any conflict of interest circumstances arise, or when there is doubt regarding possible conflict of interest, you shall disclose the same in writing with details to your immediate supervisor and / or your HR representative.

ii. Receiving and giving Gifts and Entertainment

We believe that business relationships founded on trust and mutual interest are vital to our success. We believe in conducting ourselves honestly, responsibly and fairly in our interactions with everyone including our customers, contractors and suppliers.



- a) Members should not accept any offers, payment, promise to pay any money, gift or anything of value from associate, customer, vendor, other members etc that is perceived as intended, directly or indirectly, to influence any business decision or any commitment of fraud.
- b) Inexpensive gifts, infrequent business meals etc do not violate this Code provided they are not excessive or create an appearance of impropriety.
- c) Gifts given by Members to business associates or received from them should be appropriate to the circumstances and should never create an impression of impropriety.
- d) We would encourage members to build long-term relationships with suppliers, vendors etc. so as to derive business benefit in the long-term. Members should ensure that gifts or entertainment in this regard are appropriate to the circumstances.

Some examples of appropriate gifts:

- Meals: modest occasional meals with someone with whom we do business
- Entertainment: occasional attendance at ordinary sports, theatre and other cultural events
- Gifts: gifts of nominal value, such as pens, calendars, or small promotional items.

Some examples of gifts those are clearly inappropriate:

- Any gift or entertainment that would be illegal (against the law of the land)
- Gifts or entertainment involving parties engaged in a tender or competitive bidding process
- Any gift of cash or cash equivalent (such as gift certificates, loans, stock, stock options)
- Any gift or entertainment that is a 'quid pro quo' (offered for something in return)
- Any entertainment that is indecent, sexually oriented, does not comply with the organization's commitment to mutual respect or that otherwise might adversely affect its reputation.
- A gift or entertainment that you pay for personally to avoid having to report or seek approval for, a specific action.

You will use your own discretion to use the gifts received which are appropriate, due to your role in the Company, for / in the Company.

In case of any doubt and / or if unable to classify the gift received, you will seek guidance from the immediate supervisor and act appropriately.

In case an inappropriate gift is offered or received, you will return and / or intimate the same to the concerned party immediately, as is applicable in conjunction with this Code. You will also report the same to the immediate supervisor.

iii. Bribery

You will always encourage meritocracy and shall follow it as a principle while interfacing with others including other members, government officials, business associates, contractors, agents etc. Therefore, giving or receiving an undue reward / bribe or anything to influence the behaviour of someone to obtain commercial advantage is discouraged.

Please note that in India, under the Prevention of Corruption Act, 1988, or under the applicable legislation in your jurisdiction giving of bribe to governmental officials and agents whether directly or indirectly, is strictly prohibited. As a law abiding Member, you will not directly or indirectly pay any bribe to any other Members, Governmental officials, business associates, contractors, vendors, agents, etc.

iv. Working with Associates



Marico's associates play a critically important role in our ability to operate and provide products and services to our customers. That is why we must choose them carefully, based on merit, and with the expectation that our associates will act consistently with our compliance and ethics requirements.

- a) You will choose an associate on merit; avoid conflicts of interest, inappropriate gifts and entertainment or any other kind of favouritism that might compromise or influence selection
- b) You will seek to do business with associates who comply with legal requirements and who act in a manner that is consistent with Marico's commitment to compliance and ethics as outlined in this Code
- c) You will help our associates understand our compliance and ethics requirements
- d) You will always deal fairly, ethically and lawfully with associates and customers.

"Associate" is any external person / body of persons / company / organisation we do business with. They could be advertising agencies, distributors, consultants, vendors, suppliers, third party manufacturers, etc. A separate set of guiding principles governing our relationship with our associates, known as Marico Code of Business Ethics (MCOBE) is provided as an annexure to this Code of Conduct. This would be appended to all our agreements with the associates and compliance with the same is mandatory for our continued association with such third parties. Any deviation in complying with MCOBE would be treated in the same manner as breach of Code of Conduct and the consequences to follow.

Please note that additional rules regarding associates may apply to a particular job, you are expected to get such additional rules (if any) from your supervisor and / or HR representative.

v. Compliance with laws of the land



- a) You will comply with all the applicable laws, regulations, rules and regulatory orders.
- b) You will acquire appropriate knowledge of the requirements relating to your duties sufficient to enable you to recognise potential dangers and to know when to seek advice from your supervisors, HR representatives or Legal department on specific law or company policies and procedures.
- c) Violation of any law, regulations, rules and orders may make you liable for criminal or civil action, in addition to any disciplinary action that the Company may take against you for such violation.
- d) You will not at any time or under any circumstances enter into an agreement or understanding, written or oral, express or implied with any competitor concerning prices, discounts, other terms or conditions of sale, profit or profit margins, costs, allocation of products or geographic markets, allocation of customers, limitations on production, boycotts of customer or suppliers, or bids or the intent to bid or even discuss or exchange information on these subjects. These prohibitions are absolute and strict observance is required.



Marico's Code of Conduct (CoC)

YOUR RESPONSIBILITIES

COMPANY ASSETS CONFIDENTIALITY AND FINANCIAL INTEGRITY



Treat it like it
belonged to you
... carefully





COMPANY ASSETS CONFIDENTIALITY AND FINANCIAL INTEGRITY

i. Accurate and complete data, records, reporting and accounting

You will provide to all stakeholders and other Members information that is correct and complete.

For example:

- a. Financial data (e.g. books, records and accounts) must conform both to generally accepted accounting principles and to the Company's reporting policies
- b. Information provided for employment records should be factual and accurate in all aspects.



You will treat all information that is not in the public domain (not on the Company's annual / quarterly report, published in the internet / intranet) with care. Any information stated as confidential explicitly should be treated as such.

You will not misuse and / or misappropriate the funds of the Company in any manner.

For other information where there is a doubt, you will check with the immediate supervisor or HR representative. You will not use any confidential information of the Company to accrue personal gains.

You will use Claims Against Self Authorization (CEASE), where applicable, with responsibility and integrity. You are required to read and understand the CEASE guidelines available on Company intranet/ Mera Milaap.

In line with our values of trust and openness, we will be forthright and transparent about our operations and performance, accurate in the recording and reporting of data and results, and exercise care in the use of our assets and resources.

ii. Usage of Company Assets

Company assets includes all assets including but not limited to work stations, electronic devices / equipments, materials and resources, company's intellectual property rights, software, confidential / proprietary information, facilities like internet, air conditioning, toasters, beverage vending machines, etc.

You are responsible for the proper use of the Company assets at your disposal including those provided to you for the performance of your job / work by the Company. You must safeguard such properties / asset(s) against loss, damage, misuse or theft.

You agree to use the Company properties / asset(s) only for the purpose for which the same has been provided to you and not for any other purpose. You will ensure that the Company asset is not abused or wasted.

All members are responsible for using good judgment to ensure that organization assets are not misused or wasted.

iii. Electronic Usage



You must utilize electronic communication devices made available to you in the manner in which such devices are meant to be used and for the purpose for which the same has been provided to you. You will be responsible for the fair and proper use of all electronic communications devices within the Company, including computers, e-mail, connections to the Internet, intranet and extranet and any other public or private networks, voice mail, video conferencing, facsimiles, and telephones. Posting or discussing information concerning the Company's services or business on the Internet without the prior written consent of the Supervisor, Head – Investor Relations and Head – Corporate Communications is strictly prohibited. Any other form of electronic communication used by Members currently or in the future is also intended to be encompassed under this Code. It is not possible to identify every standard and rule applicable to the use of electronic communications devices. Members are therefore encouraged to use sound judgment whenever using any feature of our communications systems. For more details please read and understand Marico's Information Security Policy(Annexure IV).

iv. Insider trading

The Company follows a strict policy on Members' share dealing rules.

Please read and understand the "MARICO EMPLOYEES (DEALING IN SECURITIES & PREVENTION OF INSIDER TRADING) RULES, 2012 (Annexure V) for greater details. You shall at all times abide by the said Rules.

v. Confidentiality

Confidential information shall include but not be limited to all undisclosed financial data or information, strategic business plans, product architectures, source codes, product plans and road maps, proprietary and technical information, intellectual properties viz. trade secrets, trade marks, patents, etc., employee details, list and names of suppliers, vendors, dealers, financial information and projections, price sensitive information, non-public information and such other information which will be specifically termed as "Confidential Information".

Members shall at all time protect the Confidential Information and shall not disclose Confidential Information to any person.

vi. Information Security



In order to maintain, secure, and ensure legal and appropriate use of the Company's information technology infrastructure, the members are required to follow, adhere to and comply with the Information Security Policy, forming part of this Code of Conduct (Annexure IV).



Marico's Code of Conduct (CoC)



YOUR RESPONSIBILITIES WORKPLACE INTEGRITY



MATTERS OF
THE HEART
... can cause flutters
at the workplace



WORKPLACE INTEGRITY

i. Equal Opportunity Workplace

Marico is committed to building a work environment of mutual trust, where all members are treated with dignity and respect. Members will be recruited, selected, developed, transferred and advanced basis our principle of meritocracy – requirements of the role and business.

You will treat all other Members of the Marico with dignity, courtesy, respect and with equality irrespective of race, colour, religion, gender identity, age, national origin, sexual orientation, marital status, physical disability, etc.

You will not abuse your position and influence other Member for committing any type of offence.

ii. Harassment-Free Workplace



Marico stands committed to maintaining a work environment free from all forms of harassment and discrimination for all members consistent with its commitment to conduct its business in accordance with principles of equality, equal opportunity, and human rights.

A key manifestation of a pleasant and conducive work environment is respect for the individual, irrespective of the gender, disability or religious orientation of the member concerned. In order to sustain this strongly through creation of a better understanding, behaviours that go against mutual respect have been articulated.

Marico Limited aims to:

- Promote appropriate standards of conduct at all times
- Encourage the reporting of behavior which breaches the Guidelines on Prevention of Sexual Harassment
- Provide an effective procedure for complaints based on the principles of natural justice
- Treat all complaints in a sensitive, fair, timely and confidential manner
- Guarantee protection from any victimization or reprisals
- Implement training and awareness - outlining strategies to ensure that all members and associates know their rights and responsibilities.

Create a working and learning environment that is free from harassment and where all individuals associated with Marico Limited are treated with dignity, courtesy and respect

You will never indulge in any act which is inconsistent with the principles of equality, equal opportunity and human rights.

You will read, understand and abide by the Prevention of Sexual Harassment at Workplace Policy annexed with this Code marked as ANNEXURE I

iii. Abuse - Substance or Alcohol

You will not use or be in possession or under influence of alcohol or illegal drugs or any other controlled / prohibited substance / material in the work place on the job or during working hours.

In case you need to use / possess any such substance under medical prescription, then you shall immediately inform your Supervisor and HR representative.

iv. Abuse of Position / Designation - Bullying

You will not abuse your position in the Company to gain any illegal advantage or for committing any offence.

Bullying is unreasonable behaviour that is directed against an individual or group; by another individual or group and is derived from the misuse of power over the target of the behaviour. This may include:

- verbal abuse, shouting
- excluding or isolating behaviour
- deliberately withholding information vital for effective work performance
- giving employees impossible assignments
- physical abuse.

It is the responsibility of all Members to ensure that premises and facilities are free from harassment, every Member has a responsibility to meet this requirement.

Bullying is unreasonable behaviour derived from misuse of power. It is unacceptable conduct and all reported incidents will be investigated

v. Racial and Religious Vilification

Racial and religious vilification is conduct that incites hatred against, serious contempt for, or revulsion or severe ridicule against a person or group on the grounds of racial identification or religious belief or activity. Racial and religious vilification is a form of harassment and discrimination and is unacceptable conduct in the Company.

vi. Respecting Privacy & Confidentiality of Members



You are expected to respect the privacy of other Members and safeguard the confidentiality of information that Marico or you had about such member. You shall comply with any and all local and international privacy and data protection laws.

Guidelines :

- a) Information pertaining to a member must be obtained only with prior consent of such Member;
- b) Members personal information gathered must be reasonable, relevant and not be intrusive in relation to the purpose for which it is collected. Such information shall only be used for the purpose for which it is collected and shall not be retained longer than necessary.
- c) All member personal information shall be kept confidential and secure.
- d) Advice must always be sought from Legal Function before gathering any personal information of a member or moving such information gathered outside the country of origin.

vii. Dress Code

Members are expected to dress appropriately during working hours or when representing the Organisation. This means presenting yourself in a professional, business appropriate style at all times. In addition you must ensure that your attire does not present a safety issue.

viii. Internet Social Media Policy

You shall not represent the Company or any brand of the Company without prior written approval from your Supervisor, Head of such Brand in any blog site, social networking site, micro blog sites, photo / video sharing sites, chat rooms, chatting sites or alike. You will also adhere to the Marico's Information Security Policy in this connection.





Marico's Code of Conduct (CoC)



GRIEVANCE REDRESSAL MECHANISM



SPEAK UP -

Today
before it's too late!



GRIEVANCE REDRESSAL MECHANISM

1. Various contact points

If you have a question or concern about legal or ethical standards, you can choose to reach out to multiple members in the Company who will be equipped to help you resolve your concern. You have the following options for reaching out.

- 1) Complaint Drop Box – installed at all Marico locations
- 2) Email your query or complaint at – speakupmarico@ethicshelpline.in
- 3) Call on toll free number - 180030000087 (For India)
- 4) CoC Website - <http://www.in.kpmg.com/ethicshelpline/marico/>
- 5) Personally contact – any Member of Code of Conduct Committee, HR Committee, Whistle blower committee
- 6) Your Line management is usually a good place to start with a legal or business conduct issue who shall inform the Code of Conduct committee.
- 7) Your HR representative who shall inform the Code of Conduct committee.

The access to Complaint drop box, email, complaints lodged through toll free number will be with CFO & CHRO.

In case of a concern on Sexual harassment, in addition to the above touch points, you also have the option of contacting any member of the PoSH (Prevention of Sexual Harassment) Committee. The names of the members are mentioned in Annexure II.

If you observe behaviour that concerns you, or that may represent a violation of the Code or any law, raise the issue promptly. Doing so will allow the Company an opportunity to deal with the issue and correct it, ideally before it becomes a violation of law, security or the Company's reputation.



2. Administration and Governance of the Code

- 2.1 The Company has constituted a Committee which will also be known as "Code of Conduct Committee" ("CCC").
- 2.2 Members to CCC will be appointed in the manner as specified under Annexure II.
- 2.3 CCC will have following Sub-committees namely:
 - a) HR committee - objective of this committee is to appoint investigation team for investigation for HR related concerns / complaints
 - b) IT Committee - objective of this committee is to implement the IT policy and resolve IT related concerns and complaints under the Code of Conduct.
 - c) Whistle blower Committee - objective of this committee is to appoint investigation team for investigation for whistle blower complaints
 - d) Prevention of Sexual Harassment Committee (PoSHC) - objective of this committee is to administer the PoSH policy in providing a harassment free work environment including but not limited to appointment of investigation team for investigation of sexual harassment complaint.

3. Role and functions of HR & IT Committee

- 3.1 HR Committee & IT Committee will primarily deal with complaints / concerns relating to issues in the domain of HR and IT respectively;
- 3.2 CCC on receiving complaint in connection with HR or IT, as the case may be or if CCC has reason to believe that there is any violation of any discipline or breach, then it will promptly divert such complaints to HR Committee or IT Committee, as applicable.
- 3.3 HR Committee & IT Committee may also receive complaints / concerns directly or indirectly.
- 3.4 HR Committee & IT Committee shall report to CCC.
- 3.5 All complaints / concerns shall be recorded and investigated and shall be submitted to CCC before the quarterly meetings of CCC and as and when called for by the CCC.

4. Role and functions of Whistle Blower Committee

- 4.1 Whistle Blower Committee will primarily deal with complaints / concerns relating to the Company Assets and / or Financial Integrity.
- 4.2 CCC on receiving complaint related to Company Assets and / or financial integrity or if CCC has reason to believe that there is any violation of any discipline in connection with Company Assets and / or financial integrity, then it will promptly divert such complaints to Whistle Blower Committee.
- 4.3 Whistle Blower Committee may also receive complaints /concerns directly or indirectly.
- 4.4 Whistle Blower Committee shall report to CCC.
- 4.5 All complaints /concerns shall be recorded and will be submitted to CCC before the quarterly meetings of CCC and as and when called for by the CCC.



5. Role and functions of Prevention of Sexual Harassment Committee

- 5.1 PoSHC will primarily deal with complaints / concerns relating to sexual harassment at workplace.
- 5.2 CCC on receiving complaint related to sexual harassment or if CCC has reason to believe that there is any incident of sexual harassment, then it will promptly divert such complaints to PoSH.
- 5.3 PoSHC may also receive complaints / concerns relating to sexual harassment directly or indirectly.
- 5.4 PoSH shall report to CCC.
- 5.5 All complaints / concerns shall be recorded and will be submitted to CCC before the quarterly meetings of CCC and as and when called for by the CCC.
- 5.6 PoSHC will also be responsible for adhering to the compliance requirements as per the PoSH policy in overseeing conciliation, training and cascading and filing of statutory returns to the government authorities, as may be applicable.



6. Broad Principles of CCC

CCC along with its sub-committees will operate on the following principles:

- a) Confidentiality,
- b) Impartiality,
- c) Promptness,
- d) Sensitivity,
- e) Courtesy and
- f) Respect

7. Reporting of Grievances & Redressal

CCC will report directly to the Corporate Governance Committee, and the Corporate Governance Committee shall report to the Audit Committee of the Company.

All sub-committees under CCC shall report to CCC.

Chairman of CCC shall be responsible to submit / file such reports / forms / returns as may be directed by the Government from time to time under any law for the time being in force.

8. Responsibilities of CCC

- 8.1 Administering, implementing and overseeing ongoing compliance under the Code.
- 8.2 Establishing, amending where necessary and administering procedures to assure that reports of Improper Activities will be collected, reviewed promptly, treated or resolved in an appropriate manner, and retained.
- 8.3 Making himself or herself available to discuss with Member(s) any complaints raised or reports filed personally with such CCC Member or otherwise.
- 8.4 Notifying the sender and acknowledge receipt of the reported violation or suspected violation. All reports will be promptly investigated and appropriate corrective action shall be taken.
- 8.5 Establishing, amending wherever necessary and administering procedures that enable Member(s) to submit reports of Improper Activities and related concerns in a confidential or anonymous manner.
- 8.6 Ensuring that the Members who are responsible for preparing and reviewing the Company's statutory filings and other public disclosures are made aware of reports of Improper Activities involving the Company's accounting, auditing, and internal auditing controls or disclosure practices.
- 8.7 Convene periodic training programs / workshops for all Members across all locations to educate them and to keep them updated with any new external development / amendments / changes in connection with the Code / applicable Laws.

- 8.8 In case any Member of sub-committee has reason to believe that there is any violation of the Code / law, then in such situation, such Member should promptly inform in writing any Member of CCC or CFO of such incident and then after obtaining directions of CCC, conduct investigation.
- 8.9 Provide directions, instructions and assistances to all sub-committees.

Other Responsibilities:

CCC shall submit its quarterly report along with summary of all meetings held, all pending Code investigations and final Code decisions, including disciplinary actions taken to Corporate Governance committee of Marico's Board of Directors and Audit Committee of the Company.

CCC will also post a representative sample of Code violations, while protecting the identity and privacy of the individuals involved, on the Ethics intranet site for the education of Members.

9. Modifications

CCC shall continuously review and update this Code and procedures. Any amendment of this code or any decision to exempt the application of any part of the code to any section of the Company - must be approved in writing by the Corporate Governance Committee of Marico's Board of Directors and promptly disclosed on the Company's website and in applicable regulatory filings pursuant to applicable laws and regulations, together with details about the nature of the amendment or waiver. THE CCC may, upon application by any Member or Suo moto issue any clarifications in respect of the code. Such clarifications shall be binding on the Company and the member. All clarifications issued shall operate prospectively and retrospectively unless expressly stated otherwise in such clarification.

10. Meetings of CCC

- 10.1 CCC shall meet as and when necessary, but at least four times in a year; ideally at the start of each quarter to review / report matters / issues of the last quarter.
- 10.2 Proceedings of all meetings shall be recorded within ten (10) days of the meeting. Such recorded proceedings will be available with Secretary of CCC.
- 10.3 Proceeding of such meeting will be reviewed and submitted to Corporate Governance Committee of Marico Limited.
- 10.4 All records of investigation / proceedings / records pertaining to any case / complaint will be kept confidential.
- 10.5 Records will be maintained by Chairman of the CCC.
- 10.6 Only Members of CCC, Corporate Governance Committee and Board of Directors will have access to such records and none.

11. Quorum of CCC Meeting

- 11.1 Presence of minimum three members of CCC will be considered valid for any decisions regarding selection of investigating committee or for the presentation of findings of investigation or for deciding any case about any Code violation.
- 11.2 Any Member of CCC absent without any valid reason for more than three consecutive times for the CCC meetings may be removed and new Member may be appointed by the remaining CCC Members.

12. Maintenance of case files, records and reports

- a) All cases investigated under this Code will be maintained in a file and will be serially numbered.
- b) Each case will carry a formal closure report, which will be signed by the Chairman of CCC within 30 days of deciding the case.
- c) All case papers, investigation reports with case closure report will be physically filed with the CFO
- d) There will be an electronic storage in the folder shared amongst the CFO, Chairman and CHRO. This location shall carry e-copies of the papers physically filed with the CFO pertaining to all cases under this Code.
- e) Only the following 3 individuals shall have access to the physical or electronic copies
 - i. Chairman
 - ii. CFO
 - iii. CHRO
- f) This said system of record keeping and maintaining will be periodically audited, without such auditor getting into the contents of cases.



13. Anonymity and Confidentiality

CCC will not distinguish between any complaint / issues raised anonymously and those raised with identity disclosed

When you report any non-compliance, violation or any complaint to the CCC through any medium, you may choose to remain anonymous, although you are encouraged to identify yourself to facilitate investigation / communication.

If you make your identity known, the Committee and investigators will keep your identity confidential, consistent with conducting a thorough and fair investigation.

In case you complain / raise any issue anonymously, attempt will nevertheless be made to seek details from the anonymous complainant

CCC will not make any effort to attribute the identity of the anonymous complainant to any Member.

14. Investigations



All complaints that make out a prima facie case of violation of the Code shall be investigated. The Company may handle the investigation internally or engage expert investigators.

CCC takes all reports of possible misconduct / violation of law / Code seriously. CCC will investigate the matter confidentially, make a determination whether the Code or any law has been violated, and take appropriate corrective action.

While conducting an Investigation following any complaint, CCC will ensure it adheres to the Principles of Natural Justice namely:

- i. Both parties shall be given reasonable opportunity to be heard along with witnesses and to produce any other relevant documents
- ii. No Person will be allowed to be a judge in his / her own case
- iii. The final decision will be made after due investigation and the application of proper reasoning.
- iv. The order of the CCC shall be in writing and shall contain reasons for arriving at the decision.

Upon completion of the investigation, both parties (if the identity of the complainant is known) will be informed of the decision of CCC.

No set of rules can cover all circumstances. These guidelines may be varied as necessary to conform to local law or contract.

15. Detailed description of the Investigation Process

15.1 Gathering concerns/queries/complaints:

- Member can address a concern or query to multiple touch points. The Company is open to listen to its members at all times.
- On receiving any complaint / concern, the CCC will need to judge the concern:
 - i) If the concern does not have anything to do with this Code of Conduct, literally and in spirit, the office of the CCC will refer it to the appropriate authority that can solve the issue. E.g.: Payroll-related concerns, administration-related concerns etc.
 - ii) If the concern is related to the Code of Conduct, the office of the CCC will immediately initiate the investigation process.

All concerns regarding code violation will be directed to the Chairperson of CCC, irrespective of who receives it. Care will be taken that the first person who receives the concern does not exercise personal judgement regarding the same.

15.2 Constitution of Investigation team

CCC will constitute an appropriate investigation team, depending upon the type of complaint; within 2 weeks of receiving the complaint.

CCC will not decide any matter without thorough investigation, except on some cases where the misconduct / breach / violation of the Code or any law is apparent or the offender / defendant confesses about such misconduct / breach / violation of the Code or any law.

Investigation team may differ depending upon the type of complaint received by CCC.

16. Decision of CCC

- 16.1 CCC Members shall decide the cases about any Code violations.
- 16.2 Decision of CCC shall be final and binding upon the Members involved in a particular case.
- 16.3 CCC shall provide reasoning to its decision.
- 16.4 Presence of minimum three members of CCC will be considered valid for any decisions regarding selection of investigating committee or for the presentation of findings of investigation or for deciding any case about any Code violation.
- 16.5 In the event of any dissent within the CCC on any decision, the decision of the majority shall prevail. In the event of equal number of votes cast for and against a decision, there shall be re-voting. In the event that the re-voting also results in equal number of votes cast for and against the decision, the Chairman of the CCC shall have a casting vote.
- 16.6 CCC will table its findings to CGC every quarter.

17. Disciplinary Actions

CCC strives to impose discipline that fits the nature, gravity and circumstances of each Code violation. It uses a system of progressive discipline, issuing letters of reprimand for less significant, first-time negligent offenses. Violations of a more serious nature may result in transfer, suspension without pay; loss or reduction of merit increase, bonus or stock option award; or termination of employment without compensation. The complainant's views may be taken into consideration for this purpose.

i) No Retaliation

The Company has an unwavering policy against retaliation for raising a good-faith concern under this Code. The Company values the help of members or associates who follow this Code of Conduct and raises a concern or reports misconduct / violation. Any retaliation against a member or organization that raises an issue honestly is a violation of this Code. That a member has raised a concern honestly, or participated in an investigation, cannot be in any circumstances, the basis for any adverse employment action, including separation, demotion, suspension, loss of benefits, threats, harassment or discrimination.

The Company has an unwavering policy against retaliation. Any retaliation against a member or organisation that raises an issue honestly is a violation of this code.

Allegations of retaliation will be investigated and appropriate action will be taken. Anyone responsible for reprisals against individuals who report suspected misconduct or other risks to business will be subjected to disciplinary action up to and including dismissal.

If you believe someone has retaliated against you, or if you suspect that you or someone you know has been retaliated against for raising an ethical issue report the matter immediately to the Ethics Committee.

ii) Making False Accusations

Honest reporting does not mean that you have to be right when you raise a concern; you just have to believe that the information you are providing is accurate. Knowingly making false accusations will constitute a violation of this code and will be investigated accordingly.

The Company will protect any member or associate who raises a concern honestly

It is a violation of the Code to knowingly make a false accusation, lie to investigators, or interfere or refuse to cooperate with a Code investigation.



Marico's Code of Conduct (CoC)



ANNEXURES



NO BUSINESS IS
COMPLETE
... unless the forms
are filled in triplicate!



ANNEXURE I

Policy on Prevention of Sexual Harassment at Workplace



1. This Policy shall be known as "Prevention of Sexual Harassment at Workplace".
2. This Policy shall be applicable to all Members to whom the Code is applicable
3. DEFINITION:
 - 3.1 "Sexual harassment" includes any one or more of the following unwelcome acts or behaviour (whether directly or by implication) namely;
 - (i) physical contact and advances; or
 - (ii) a demand or request for sexual favours; or
 - (iii) making sexually coloured remarks; or
 - (iv) showing pornography; or
 - (v) any other unwelcome physical, verbal or non-verbal conduct of sexual nature;
 - (vi) The following circumstances may be deemed as sexual harassment, if it occurs or is present in relation to or connected with any act or behaviour of sexual harassment as defined above;
 - a. implied or explicit promise of preferential treatment in his / her employment / association; or
 - b. implied or explicit threat of detrimental treatment in his / her employment / association; or
 - c. implied or explicit threat about his / her present or future employment status / association status; or
 - d. interferes with his / her work or creating an intimidating or offensive or hostile work environment for him / her; or
 - e. humiliating treatment likely to affect his / her health or safety.
 - 3.2 "Workplace" means -
 - (a) any premises that is owned or controlled by the Company; it shall include company provided transportation.
 - 3.3 "Unwelcome" is the key in defining sexual harassment. It is the impact and effect of the behaviour, to the disapproval of the recipient that will define the behaviour as sexual harassment.
 - 3.4 "Relationship" implies association between two individuals out of their free will or choice as companions beyond and outside the requirements of work / profession.
 - 3.5 "Consensual Relationship" refers to intimate and close relationship between two individuals perceived to be with the consent of each other. This policy will not take cognizance of complaints from concerned members to adjudicate on such relationships as a sexual harassment issue. However, should such relationships manifest as 'conflict of interest' situation, Company reserves its right to proceed against the concerned Members as per the disciplinary proceedings under the Code of Conduct, as appropriate.

Unwelcome is the key in defining Sexual Harassment. It will always be decided by the recipient basis the impact and effect of the behaviour.



3.6 "Aggrieved Person" means a person who alleges to have been subjected to any act of sexual harassment in any workplace;

3.7 "Chairperson" means Chairperson of the Prevention of Sexual Harassment Committee (PoSHC);

4. Every case of harassment is not sexual harassment. It is the impact, effect and sexual motive of the alleged behaviour / conduct, on the victim that determines the extent and gravity of sexual harassment. Inability or reluctance of the victim to raise a sexual harassment complaint due to fear or threat of job loss or disadvantage at work and / or social stigma, will not amount to acquiescence and it will not absolve the accused from charges of sexual harassment.

We consider sexual harassment to be a gender neutral issue and accordingly a sexual harassment complaint can be made either by a man or a woman if he or she has suffered a behaviour or victimisation as spelt out above.

5. No Member shall be subject to sexual harassment at any workplace;
6. It is expected that members should be conscious and be aware of behaviours that are likely to cause discomfort to the other gender and should abstain from the same. Accordingly, irrespective of the intent, motive or the extent of proximity or friendship, the following behaviours could be perceived as sexual harassment.
- Friendship gestures suggesting intimacy, like grabbing, brushing, touching, pinching, putting the arm around the shoulder / waist, etc.
 - Increments, Promotions, employment benefits offered to a person on a 'quid pro quo' basis with an underlying expectation of sexual gratification e.g. asking for a night out, etc.
 - Passing comments with sexual connotations, making sexist remarks, vulgar descriptions around the looks, appearance, dressing sense etc. to the embarrassment of the concerned person.
 - Showing or displaying any sexually explicit visual material, in the form of pictures / cartoons / pin-ups / calendars / screen savers on computers / any offensive written material / pornographic e-mails/inappropriate sms / Whats app messages etc.
 - Engaging in any other unwelcome conduct of a sexual nature, which could be verbal, or even non- verbal, like staring to make the other person uncomfortable, making offensive gesture e.g. making kissing noise, etc.
 - Exhibitionism (flashing oneself) intentionally with a sexual innuendo.
 - Demanding and persistently asking a person out when the person asked out is reluctant and has showed lack of interest.
 - Vitiating the work environment with any of the above behaviour, since it is not objected to or has been accepted over a period of time, thereby making it hostile for the employees in general.
 - A hostile work environment can also be caused by any two members in an intimate personal relationship, if the behaviour displayed by the two members created difficulties or discomfort for others. It then becomes a 'hostile work environment' for the other members.
 - Unsolicited remarks, rumours and gossip casting aspersions on the character of a person attributing his / her career aspirations to intimate or quid-pro-quo relationship at work.



7. Raising Sexual Harassment Complaints

In case of any issues of sexual harassment nature, whether existing or perceived, either explicit or implied as per Section 3.1 above, the Aggrieved Person (or any other person on his / her behalf) is required to report the matter as early as possible - not later than 3 months, unless it is a case of ongoing harassment - to any of the following, without any order of preference -

1. Write to any Member of PoSH Committee at their designated E Mail ID or by post;
2. Submit a written complaint in the complaint drop box made available at all locations of the Company;
3. Call on toll free helpline number - 180030000087 (For India)
4. CoC Website - <http://www.in.kpmg.com/ethicshelpline/marico/>
5. Write to the HR representative or approach for guidance / support on raising the issue
6. Inform the Supervisor, (in case the complaint is not against him / her)
7. Write to any Member of CCC at their designated E Mail ID.
8. Email your query or complaint at – speakupmarico@ethicshelpline.in



Irrespective of the channel of communication, all reported matters (raised under 2-7) shall be duly forwarded to the PoSH Committee, within 3 days and not later than 7 days, for further action in the matter.

While there is no prescribed format for raising a complaint, it is recommended that the complainant shall make the complaint, along with necessary facts, documentary evidences and details of witnesses, as available for a thorough and unbiased inquiry into the matter.

8. Conciliation

While an Aggrieved Person has a right to raise a sexual harassment issue and get the matter investigated till its resolution, if for any reason, the member decides or chooses to withdraw the complaint - for reasons of social stigma or other personal reasons, the same shall be considered in accordance with the provisions of the law, and shall be dealt with as follows:

- 8.1 PoSH Committee may before initiating an investigation and at the request of the Aggrieved Person take steps to settle the matter between such Aggrieved Person and the respondent through conciliation.
- 8.2 No monetary settlement shall be made as a basis of conciliation
- 8.3 Where a settlement has been arrived at under clause 8.1 above, PoSH committee shall record the settlement so arrived and forward the same along with recommended action, to CCC to take action as specified in the recommendation.
- 8.4 PoSH Committee shall provide copies of the settlement as recorded by the committee to the Aggrieved Person and the respondent.
- 8.5 Where a settlement is arrived at, no further investigation shall be conducted by PoSH Committee.



9. INVESTIGATION

- 9.1 Issues raised under this policy shall be referred for investigation at the instance of PoSH committee as per the protocol defined under the Code of Conduct.
- 9.2 The PoSH Committee shall follow the principles of natural justice by adhering to the following steps in particular with regard to inquiry into the complaint.
- (i) Atleast 3 members of the PoSH committee (including the Chairperson) shall preside over the inquiry.
 - (ii) On receipt of the complaint, the PoSH Committee shall send a copy of the complaint to the accused Member, within 7 working days, indicating the deadline by which a response, along with evidences and details of witnesses should be submitted.
 - (iii) The accused Member shall also be given an opportunity to be heard and make written submissions on the allegations made and circumstances leading to the complaint.
 - (iv) In case of failure on the part of the Member to respond to the complaint or make himself / herself available for the hearing, the PoSH committee in its discretion may terminate the inquiry in favour of the victim, after giving 15 days' notice to the parties concerned.
 - (v) The parties shall not engage a lawyer to represent their case in proceedings before the PoSH committee.

At the recommendation of the PoSH committee, choice of location and additional witnesses as per the requirement of the victim may be considered. Details of the investigation are "Privileged and confidential" and the PoSH committee shall determine the people (including audit) and the content of findings to be made available - for the purposes of reporting to the management.



- 9.3 In case of conciliation as per clause 8.1, PoSH is authorised to conduct independent investigation, in case the terms and conditions of the settlement has not been complied with by the respondent.
- 9.4 In the event, the victim chooses to take recourse to law, the Company may at its sole discretion decide to not pursue the matter further.
- 9.5 Investigation shall be completed within a period of ninety (90) days
- 9.6 During the pendency of an investigation, on a written request made by the Aggrieved Person, PoSH, may recommend to the Company -
- a) Suspension of the Respondent or transfer of the Respondent / Aggrieved Person to any other workplace; or
 - b) grant paid leave to the Aggrieved Person upto a period of three months; or
 - c) grant such other reasonable relief to the Aggrieved Person as may be directed by the PoSH Committee - viz.
 - a restraint on the accused Member to oversee / supervise the work performance of the victim in case of direct working relationship;
 - assigning the performance evaluation to another supervisor at the discretion of the management;
 - Any other relief as appropriate.
- 9.7 The leave granted to the Aggrieved Person as above, shall be in addition to the leave he / she would be otherwise entitled.

10. Investigation Report

10.1 Investigation report along with its finding and recommendation shall be submitted to the PoSH Committee and PoSH Committee will submit the same to CCC within a period of ten days from the date of completion of the investigation in consideration of the following -

- (i) Nature of evidences in support of the allegation;
- (ii) Leading circumstances culminating into sexual harassment;
- (iii) Discrepancies, if any, in the allegations and the submission made by the victim and his / her witnesses;
- (iv) Grounds for review or counter allegations/ evidences from the accused.

10.2 In case the PoSH Committee arrives at the conclusion that the allegation against the respondent has not been proved, it shall recommend to CCC that no action is required to be taken against the respondent. However, in case the complaint is found to be false, malicious, and frivolous then such complaining Member shall be liable for disciplinary actions, including but not limited to payment of compensation to the respondent.

10.3 In case the PoSH Committee arrives at the conclusion that the allegations against the respondent has been proved, it shall recommend to CCC as the case may be

- i) to take action for sexual harassment as a misconduct in accordance with the provisions of the Code;
- ii) The punishment could range from warning, monetary penalty and counselling to termination of employment depending on the gravity of the offense and its impact on the victim.
- iii) In case of monetary fine or penalty, the PoSH may recommend for the same to be paid to the victim to defer the cost of medical treatment or for seeking professional counselling, as the situation may warrant and for this purpose, the Company is authorised to make requisite recoveries from the remuneration payable to the accused and in case of separation of the employee, for such recoveries to be made out of the final settlement.
- iv) CCC shall act upon the recommendations of PoSH committee within thirty days of receipt of final investigation report.

11. Determination of Compensation to Aggrieved Person

For the purpose of clause (iii) of 10 above, in determining the sums to be paid to the Aggrieved Person, PoSH shall have regard to -

- a) the mental trauma, pain, suffering and emotional distress caused to the Aggrieved Person
- b) the loss in the career opportunity due to the incident of sexual harassment
- c) medical expenses incurred by the Aggrieved Person for physical and psychiatric treatment
- d) the income and financial status of the respondent
- e) feasibility of such payment in lump sum or in instalments.

The Company shall have the right to withhold the dues equivalent to the awarded compensation from any dues payable by the Company to the Respondent by way of remuneration/ final settlement.



12. Powers of PoSH

12.1 For the purpose of making investigation, PoSH committee shall have the following powers:

- 12.1.1 Summoning and enforcing the attendance of any Member and examining such Member
- 12.1.2 Requiring the discovery and production of documents; and
- 12.1.3 Any other matter which may be prescribed.

13. Appeals And Revision

The decision of the CCC is final and shall not be open to any review or appeal, unless additional evidences not considered by PoSH Committee are brought on record or fresh instances emanating from past sexual harassment complaint have arisen.

The CCC in such cases may order a fresh investigation and the matter will be re-opened and pursued as an independent investigation without prejudice to the findings and recommendations of the PoSH committee,

14. Members of Prevention of Sexual Harassment (PoSH) Committee:

A designated and independent committee known as PoSH Committee will be set up, constituting the Internal Committee for the purposes of dealing with sexual harassment complaints, pursuant to this Policy. This committee will be co-opted by senior most lady manager at each location (where available) – to constitute the unit level Internal committee.

Following is the proposed membership of the PoSH Committee

- Chairperson - Senior-most lady manager
- Company Secretary and Compliance Manager / Woman manager responsible for compliance function
- Chief Human Resources Officer
- Head - Legal
- One external member familiar with women-centric issues and conversant with legal implications of sexual harassment offenses (woman).



The CCC shall monitor and oversee the working of the PoSH committee in addition to ensuring that the constitution of the PoSH Committee shall at all times conform with the requirement of minimum 50% membership and legal resource by women in the committee.

15. Training and Communication

The PoSH committee will steer a robust communication and awareness building program across the organization by undertaking the following –

- i) Display of the details of the PoSH Committee members along with contact details, reporting mechanism and the PoSH policy at conspicuous places in all locations (e.g. Visitors' Lobby, Reception area, canteen, recreation centre, etc.)
- ii) Include a module on Sexual harassment in the corporate training programs including induction courses
- iii) Conduct specialised capability building training programs for members of the PoSH committee and the investigation team members.
- iv) Make available evidences of attendance / confirmation on training for audit verification
- v) Maintain necessary log and provide details of sexual harassment complaints.



ANNEXURE II

A. Members of Code of Conduct Committee (CCC)

Sr.No	Committee Member	Designation	Email Id
1	Ashutosh Telang	Chief Human Resources Officer	ashutosht@marico.com
2	Vivek Karve	Chief Financial Officer	vivek.karve@marico.com
3	Suresh Jagirdar	Chief Legal Counsel	suresh.jagirdar@marico.com
4	Mukesh Kripalani	Chief - Business Process Transformation & IT	mukesh.kripalani@marico.com
5	Shruti Ambegaoker	Head - Organization Development	shruti.ambegaoker@marico.com
6	Swati Dwivedi	Business HR Head - Corporate Functions	swati.dwivedi@marico.com

B. Members of Prevention of Sexual Harassment Committee (PoSHC)

As defined under clause 14 of the PoSH policy.

Sr.No	Committee Member	Designation	Email Id
1	Shruti Ambegaoker	Head - Organization Development	shruti.ambegaoker@marico.com
2	Avani Mainkar	Head - Personal Care & Nature Care	avani.mainkar@marico.com
3	Swati Dwivedi	Business HR Head - Corporate Functions	swati.dwivedi@marico.com
4	Archana Singh	External Member	archana.rajn.singh@gmail.com
5	Ashutosh Telang	Chief Human Resources Officer	ashutosht@marico.com
6	Suresh Jagirdar	Chief Legal Counsel	suresh.jagirdar@marico.com
7	Ekta Sarin	Manager- Legal	ekta.sarin@marico.com

C. Representatives from locations on PoSH Committee for locations

Sr.No	Location	Name	Email Id
1	North Division - Sales & Marketing	Udita Rajadnye	udita.rajadnye@marico.com
2	South Division - Sales	Supriya Bendre	supriya.bendre@marico.com
3	East Division - Sales	Shringar Bhuwania	shringar.bhuwania@marico.com
4	West Division - Sales	Dr. Avani Mainkar	avani.mainkar@marico.com
5	MARKS Office	Dr. Avani Mainkar	avani.mainkar@marico.com
6	Kanjikode	Aby Kottukappally	aby.kottukappally@marico.com
7	Perundurai	Sreenivasan T	sreenivasan.t@marico.com
8	Pondicherry	G. Arul Anand	g.arul@marico.com
9	Jalgaon & Paldhi	Saket Saurav	saket.saurav@marico.com
10	Baddi	Surajit Dey	surajit.dey@marico.com
11	Dehradun & Paonta Sahib	Nitin Pathak	nitin.pathak@marico.com
12	Gawahati	Sankarjyoti Kakoty	sankarjyoti.kakoty@marico.com
13	Buying Office, Coimbatore	Girish Iyer	girish.iyer@marico.com
14	Grande Palladium	Shruti Ambegaoker	shruti.ambegaoker@marico.com
15	Grande Palladium	Ashutosh Telang	ashutosht@marico.com
16	Grande Palladium	Swati Dwivedi	swati.dwivedi@marico.com
17	Grande Palladium	Suresh M. S. Jagirdar	suresh.jagirdar@marico.com
18	Grande Palladium	Ekta Sarin	ekta.sarin@marico.com

D. Members of Prevention of Sexual Harassment Committee (PoSHC)

As defined under clause 14 of the PoSH policy.

Sr.No	Committee Member	Designation	Email Id
1	Shruti Ambegaoker	Head - Organization Development	shrutia@maricoindia.net
2	Dr. Avani Mainkar	Head - Personal & Nature Care, Marico India	avanim@maricoindia.net
3	Swati Dwivedi	Business HR Head - Corporate Functions	swatid@maricoindia.net
4	Archana Singh	External Member	archana.rajan.singh@gmail.com
5	Ashutosh Telang	Chief Human Resources Officer	ashutosht@maricoindia.net
6	Suresh Jagirdar	Chief Legal Counsel	sureshj@maricoindia.net
7	Hemangi Ghag	Manager - Secretarial	hemangiw@maricoindia.net

E. Representatives from locations on PoSH Committee for locations

Location	Name	Designation	Email Id
North RO	Sharika Munshi	Group Product Head - Livon	sharikam@maricoindia.net
South RO	Supriya Bendre	Area Sales Manager - Modern Trade	supriyab@maricoindia.net
East RO	Mohsin Ansari	Divisional Sales HR Manager	mohsina@maricoindia.net
West RO - MARKS Off	Dr. Avani Mainkar	Head-Personal & Nature Care, Marico India	avanim@maricoindia.net
MARKS Off	Dr. Avani Mainkar	Head-Personal & Nature Care, Marico India	avanim@maricoindia.net
Kanjikode	Boban Thomas	Employee Relations Manager	boban@maricoindia.net
Perundurai	Sreenivasan T	Plant Operations Manager	sreenivasan@maricoindia.net
Pondicherry	G. Arul Anand	HR Manager	arula@maricoindia.net
Jalgaon	Debashish Majumdar	HR Manager	debashishm@maricoindia.net
Paldhi	Debashish Majumdar	HR Manager	debashishm@maricoindia.net
Baddi	Soumya De	HR Manager	soumyade@maricoindia.net
Paonta Sahib	Harmanjit Singh	HR Manager - Value Added Hair Oil Operations	harmanjits@maricoindia.net
Dehradun	Naresh Gehlaud	Head - Value Added Hair Oil Operation	nareshg@maricoindia.net
Coimbatore Buying Off	Girish Iyer	Head - Copra Buying	girishi@maricoindia.net
Bangladesh	Sidhartha Das	Head - HR, MBL	sidharthad@maricobangladesh.net
Egypt	Edwin James	Head-HR, Middle East & North Africa(MENA)	edwinj@maricoindia.net
Dubai	Shakti Shekhawat	HR Manager	shaktis@maricoworld.net
South Africa	Prateek Singh	HR Manager - Marico International	prateeks@maricoindia.net
Vietnam	Nguyen Ngoc Anh Tuan	VP - Human Resources	tuanna@icpvn.com
Vietnam	Nguyen Thi Thu Trinh	Senior Marketing Manager	trinhntt@icpvn.com

Email | speakupmarico@ethicshelpline.in

India Toll Free No. | 180030000087



ANNEXURE III

MARICO'S CODE OF BUSINESS ETHICS (MCOBE)

This code is applicable to all our associates.

Associate means external person/body of persons / company / organisation Marico does its business with. They could be advertising agencies, distributors, consultants, vendors, suppliers, third party manufacturers, etc.

1. Ethics

To meet social responsibilities, you are expected to conduct your business in an ethical manner and act with integrity.

You shall safeguard and make only appropriate use as authorized by Marico Group of confidential information and ensure that all employees, associates, business partners privacy and valid intellectual property rights are protected.

2. Legal Compliance

- a) You will comply with all the applicable laws, regulations, rules and regulatory orders.
- b) You will acquire appropriate knowledge of the requirements relating to your duties sufficient to enable you to recognise potential dangers and to know when to seek advice from Legal department of Marico on specific law or company policies and procedures.
- c) Violation of any law, regulations, rules and orders may make you liable for criminal or civil action, in addition to termination / suspension of your association with the company without any compensation / damages for such action against you.
- d) You will not at any time or under any circumstances enter into an agreement or understanding, written or oral, express or implied with any competitor concerning prices, discounts, other terms or conditions of sale, profit or profit margins, costs, allocation of products or geographic markets, allocation of customers, limitations on production, boycotts of customer or suppliers, or bids or the intent to bid or even discuss or exchange information on these subjects. These prohibitions are absolute and strict observance is required.

3. Prohibition of Corruption & Bribery

You warrant that you will not make any payment, gift or other commitment to Members of Marico group, to Government officials or otherwise in a manner contrary to applicable laws, policies or standards of conduct, for the purpose of obtaining or facilitating the performance of or otherwise relating to the contract.

Nothing in this Policy will render Marico liable to reimburse the vendor / associate / agents or their associates for any such consideration given or promised or for any consequences arising out of such actions.



4. Labour and Human Rights

You shall comply with all laws including specifically, the labour laws. In case of any discrepancy between Marico's understanding or interpretation of law and yours, please note that for decision on violation of this Code, Marico's interpretation of law shall apply.

You will ensure that the work environment provided by you to your employees / staff is free from all types of harassment.

5. Health & safety of the employees / staff

You will provide a safe and healthy working environment for all the employees / staff working at your office / factory.

6. Environment Protection

It is essential that you will have to comply with all applicable environmental regulations. All required / applicable permits, licenses, information registrations and restrictions shall be obtained by you.

You will not use any form of forced, bonded or child labour. You are expected to protect the human rights of your employees / staff and to treat them with dignity and respect.



ANNEXURE IV

TABLE OF CONTENTS

Information Security Policy

1	Introduction	41
2	Title And Objective	41
3	Definitions	42
4	Commencement, Applicability And Breach	44
5	Modifications To The Policy	45
6	Guidelines For Providing Suggestions On The Policy	45
7	General Restriction	45
8	Responsibilities Of Members	45
9	Policy Pertaining To Electronic Mail	46
10	Policy For Internet Usage	48
11	Dial-in-access ("VPN") Policy	49
12	Protection Of Information	50
13	Laptop / Desktop Usage Policy	53
14	Software Usage, Maintenance And Monitoring	54
15	Wireless Communication Policy	54
16	Due Diligence Measures	55
17	Indemnity By Members	56
18	Enforcement	
18.1	Constitution Of IT Committee	57
18.2	Anonymity And Confidentiality	57
18.3	Various Options To Reach IT Committee	57
18.4	Investigations	57
18.5	Compliance	58
19	Penalty	58
20	Severability	58
21	Amendment	58
22	Affirmation Of Acceptance And Acknowledgement	
	Annexure I - System Asset Requisition Form	60
	Annexure II - Gate Pass Card For Issuing Portable Assests	61
	Annexure III - Data Protection Policy	63
	Annexure III (A) - Personal Information Consent Form	66

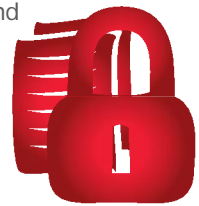


ANNEXURE IV

Information Security Policy

1. Introduction

- 1.1 This Policy shall form part of each Member's terms of employment / association along with the appointment letter issued to or the agreement entered into with him / her.
- 1.2 The Company is committed to protecting the confidentiality of personal information relating to the Members. The Members understand and agree that certain personal information is required by the Company for operational purpose and have accepted to let the Company have access and the right to use such information.
- 1.3 The Company is committed to the protection of the information assets and information technology resources that support its operations globally. The Company's scale of operations necessitates exchange and transmission of humungous information, sensitive or otherwise, electronic or otherwise on a day to day basis.
- 1.4 Without the implementation of appropriate controls and security measures, these resources are subject to potential damage or compromise to confidentiality or privacy, and thus disrupting the activities of the Company as well as of individual Member.
- 1.5 The purpose of this Policy is to maintain, secure, and ensure legal and appropriate use of the Company's information technology infrastructure. The Company's policy seeks to place security and privacy policy specifics in service of each other in order to provide Members with a high quality, trusted and secure computing environment, and as a means of protecting and securing its assets interests, data and intellectual property.
- 1.6 This Policy shall substitute previous Policy(ies) pertaining to Information security.



2. Title and Objective

- 2.1 This Policy shall be called as "Information Security Policy". Herein after to be referred to as "this Policy"
- 2.2 The obligations set out under this Policy are mandatory and shall be enforceable between the Company and for Member/s.
- 2.3 Objective of this Policy
 - 2.3.1 to prevent unauthorized disclosure of information
 - 2.3.2 to prevent unauthorized, deliberate alteration of information
 - 2.3.3 to prevent unauthorized, deliberate destruction or deletion of information and prevent practices which obstruct or degrade the usability of the information technology resources
 - 2.3.4 safeguard against situations wherein the Company could incur legal liabilities due to unacceptable actions of its Members
 - 2.3.5 to comply with all applicable regulatory and legislative requirement

2.4 Members shall:

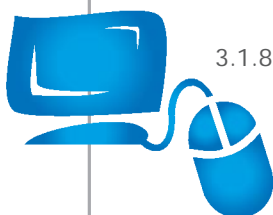
- 2.4.1 keep themselves abreast of the physical security and authentication rules in accessing the information systems authorized for use
- 2.4.2 adopt additional vigilant security practices while using mobile devices (like Laptops, Smart Phone, mobile phones etc)
- 2.4.3 secure individual passwords and not sharing them
- 2.4.4 use the facility for the Company business purposes only
- 2.4.5 restrict instant messaging only for the Company business purpose and not to send / receive text / audio / video file to any other person
- 2.4.6 use centralized file share facilities to store data where possible, and limit copies on local storage / removable media
- 2.4.7 not download content / software / material indiscriminately from unknown sources / restricted / abandoned site either directly or indirectly through the Company's IP address without express permission / approval from IT Committee.



3. Definitions

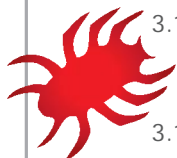
3.1 In this Policy, unless the context otherwise requires:

- 3.1.1 "Access", with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical arithmetical or memory function resources of a computer, computer system or computer network
- 3.1.2 "Applicable Law(s) / Law" includes any laws laid down by a Competent legislature, decisions of Judicial form having a binding effect and national or international treaties that have a binding effect
- 3.1.3 "Associate" means a Person who or which has access to or use of, either directly or indirectly, the Computer Resource of the Company and includes consultant, contractor, supplier, vendor, distributor, third party manufacturer, any other business associate by whatsoever name called
- 3.1.4 "Confidential or Proprietary information" shall have same meaning as defined in terms of employment or association
- 3.1.5 "Communication" means dissemination, transmission, carriage of information or signal in some manner and includes both a direct communication and an indirect communication
- 3.1.6 "Company" means Marico Limited its Subsidiary Companies and joint ventures
- 3.1.7 "Company asset" includes Company owned information, Data, Device, Information system, Computer Network, Computer System, Computer Resource
- 3.1.8 "Computer" means any electronic, magnetic, optical or other data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to computer in a computer system or computer network;
- 3.1.9 "Computer network" means the interconnection of one or more computers through -
 - (i) the use of satellite, microwave, terrestrial line or other communication media; and
 - (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained



- 3.1.10 "Computer resource" means Computer, Computer System, Computer Network, Data, computer data base or software
- 3.1.11 "Computer system" means a Device, including input and output support Devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions
- 3.1.12 "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the Computer
- 3.1.13 "Device" means any electronic, electromechanical, electro magnetic optical or other instrument, machine or component, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument and computer system, to view or to inspect or to listen to or record or transmit any information or data and includes a collection of devices
- 3.1.14 "Grievance Officer" means Head - IT Infrastructure
- 3.1.15 "HOD" means Head of Department, by whatever designation known
- 3.1.16 "Information" includes data, text, images, sound, voice, codes, computer programmes, software and database or micro film or computer generated micro fiche
- 3.1.17 "Information system" means all hardware and software assets of Marico that store, process or transmits data / information of the Company and includes servers, email, SAP, MI-Net and other applications, programs, desktops, laptops, network elements like routers, switches, firewalls
- 3.1.18 "IT personnel" includes a Member entrusted with the responsibility of developing, maintaining and safe guarding Information Technology systems and solutions for the Company
- 3.1.19 "Joint Venture" means a contractual arrangement whereby two or more parties undertake an economic activity, which is subject to joint control
- 3.1.20 "Member" means a person who is -
1. an employee whether part-time or full-time, fixed term, permanent trainee; or
 2. an individual who is a temporary staff, intern, secondee, an apprentice; or
 3. a third party or parties who represent the Company or act on behalf of the Company; or
 4. an employee of Joint Ventures where the Company has management control; or
 5. an employee of new acquisitions; or
 6. an Associate
- 3.1.21 "Official purpose" means the purpose for which any information, data or computer resource is provided to a Member in furtherance of fulfilment of his / her professional commitment towards the Company





- 3.1.22 "Person" includes an individual, any company or association or body of persons, whether incorporated or not
- 3.1.23 "Personal device" means any device which is not provided by the Company
- 3.1.24 "Subsidiary" shall have same meaning as defined under section 4 of the Companies Act, 1956
- 3.1.25 "SOP" means Standard Operating Procedures
- 3.1.26 "Virus" means a program that has the capability to spread by replicating itself to destroy, damage, degrade or adversely affect the performance of the computer resource that requires some user action to trigger it off
- 3.1.27 "Virtual Private Network (VPN)" means a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the Company's computer network
- 3.1.28 "Worm" means a program that has the capability to spread by replicating itself to destroy, damage, degrade or adversely affect the performance of the Computer Resource that propagates in accordance with its own inbuilt logic without any action from the user.

3.2 Interpretation:

- 3.2.1 Save to the extent that the context or the express provisions of this Policy otherwise require:
 - 3.2.1.1 headings and sub-headings are for ease of reference only and shall not be taken into consideration in the interpretation or construction of this Policy;
 - 3.2.1.2 all references to clauses and Annexure are references to clauses of, Annexure to this Policy;
 - 3.2.1.3 Annexures to this Policy are an integral part of this Policy and reference to this Policy includes reference thereto and reference to any Annexure includes reference to any Annexure or Appendix thereto;
 - 3.2.1.4 any reference in this Policy to any law or any provision thereof shall, in relation to an area in which such law or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area;
 - 3.2.1.5 words importing the singular include the plural and vice versa;
 - 3.2.1.6 words importing a particular gender include all genders;
 - 3.2.1.7 the term "including" means including but without limitation;
 - 3.2.1.8 expression in the present time shall mean a reference also to the past or future time and vice versa;

4. Commencement, Applicability and Breach

- 4.1 This Policy shall come into effect from 25th March 2014.
- 4.2 Applicability:
 - 4.2.1 This Policy is applicable to all the Members.
 - 4.2.2 To the extent this Policy conflicts with Applicable Law, the Applicable Law shall prevail.
- 4.3 The obligations set out under this Policy are mandatory.
- 4.4 Breach of any of the obligations, by a Member shall invoke the penalty and indemnity clauses as contained in the Policy.

In the event of any notice of non-compliance under this Policy, the burden of proof of compliance shall be that of the Member.

5. Modifications To The Policy

5.1 Marico Limited reserves the right to modify these guidelines from time to time. Any changes to this Policy shall be duly communicated to all Members through appropriate channels and would be effective and shall be binding on the Members.

6. Guidelines for Providing Suggestions on this Policy

6.1 If any Member has any doubts about this Policy or wishes to make any comments or suggestions regarding these guidelines, you can email us at infosecurity@maricoindia.net or contact: Mr. Satish Pai, Head - IT Infrastructure (Grievance Officer).

7. General Restriction

7.1 Any Device including any personal Device or Device which is provided by the Company, which is, or has been, engaged in any Communication with or without attachment(s) in respect of any Company information and / or Data; in course of employment or association with the Company will be deemed to be Company asset.

7.2 It is hereby clarified that any Communication through such Device whether such communication is made during office hours or otherwise and / or on a holiday or on working day will be deemed to be made for "official purpose".

7.3 The Company shall have the right to access, copy, share, transfer, remove, and delete, all Information / Data on Device that is used by a Member for official purpose.

The individual waives his right to privacy in respect of any personal data including photos / files etc stored on the device.

8. Responsibilities of Members

8.1 Member should read, understand and comply with this Policy.

8.2 Member may make a requisition for Company asset only in the form specified in Annexure I if such Company asset is required to carry out the entrusted functions. The Member should clearly mention the purpose for the usage of the Company asset. Such form needs to be approved by HOD of respective departments.

8.3 Laptop may be provided to a Member in Manager grade and above or to a Member in any other grade, after approval from their respective HOD & Head IT.

8.4 All Members will follow a standard Computer configuration Policy as provided by the Company across the globe. Any deviation in this configuration will require approval of respective MD & CEO.

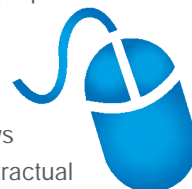
8.5 Existing laptop of the Member will be able to get a replacement only after defined period. Currently 4 years through proper approval process. After 4 years, laptop reaches "Technical End of life" and also becomes un-manageable in terms of getting spare / support.

8.6 Members shall hand over the laptop computer at the end of its technical life to the company.

8.7 Member should ensure that they are aware of, and understand, the security procedures for the specific Computer Systems they use.




- 8.8 Member should take all reasonable precautions to protect Information Systems against unauthorized access, use, disclosure, modification, duplication or destruction of computer, Computer Network, Computer System, Device, Information System.
- 8.9 Member should use Information Systems only as may be necessary for their job responsibilities.
- 8.10 Member should use available mechanism and procedures to protect their own Data and Data under their control.
- 8.11 Member should take back up of critical information and data in the desktop / laptop regularly at least once a week using company provided software.
- 8.11 Member should assist and co-operate in the protection of the Computer Systems they use.
- 8.12 Member should use Information Systems in compliance with Applicable Laws relating to electronic activity, confidentiality, copyrights, licenses and contractual obligations.
- 8.13 Member should report security problems / threats or issues to respective supervisors, systems administrator or help desk as may be appropriate.
- 8.14 Member should make an entry of information (like machine and adaptor serial number) of temporarily issued laptops in "Gate Pass Card for Issuing Portable Assets" at the time of entry to and exit from the offices of the Company. The form is enclosed in Annexure II.
- 8.15 The Members shall be solely responsible for the physical security of the devices provided by the company. In the event of loss of Laptop Computers other than due to the negligence of the Members, the Company shall provide a replacement, loss of Laptop Computers more than one shall be deemed to have been caused due to Member negligence. Save and accept the above, loss of all Devices shall be replaced by the Member at his cost.
- 8.16 Member should ensure that the desktop provided to him / her is handled with proper care. To shift the desktops, Member need to log a call with local helpdesk, who will co-ordinate with Admin Department for shifting the Desktop.
- 8.17 On separation from the services / association of / with Marico, Members should submit to the IT department email Member-ids, application Member-ids, materials, software, hardware, desktop / laptops etc that have been provided to the Member to carry out his / her job.



9. Policy Pertaining to Electronic Mail

- 9.1 Members shall be provided with access to computing resources through any Device shared or for exclusive use depending upon the nature of work and level of the Member in the Company.
- 9.2 Members shall be provided with official email address with permission to receive and send internal and external mail.
- 9.3 Mail and Mailbox size on mail server shall be decided by the IT Committee from time to time and communicated to the Members. Request for relaxation of mailbox size shall be considered by the IT Committee, subject to approval by the HOD.

- 9.4 All temporarily associated Members will be provided with email ids to send internal mail on request from HOD of relevant department. Permission to send external mail will be given on recommendation by concerned department to IT.
- 9.5 The Company may monitor, inspect, disclose the content of any Member in the business interests; or required under any law or order of the Court or any Statutory authority(ies); or when there is reasonable ground to believe that Information Security Policy is being violated, or have been violated. 
- 9.6 Any deviation to this Policy will require written or email authorization from such Member's HOD and HR HOD.
- 9.7 Acceptable Use:
- 9.7.1 Email is permitted primarily for official purposes with limited personal use only. It is however advisable that personal email ids be used for non official mail.
 - 9.7.2 Use of official email ids for subscription to newsgroups, interest groups, social networking sites, blogging sites or any mode of communication through internet will be strictly as per provisions of this Policy. This does not include sites initiated by the Company namely Kwench, TSR Darashaw etc. Official email ids can be given to Banks / finance companies etc. for enabling transactions. Official Email ids can also be used for receiving communications on topics related to official business.
 - 9.7.3 No Communication for official purposes shall be routed through any means other than through Company provided Devices, Computer Resources, Computer Networks, Email Addresses. In case any personal email id is required to send mail in cases of emergency, this use shall be reported to the HOD and IT Committee within 3 days. This relaxation shall not apply to any person serving notice period.
- 9.8 Unacceptable Use:
- 9.8.1 Transmitting internal, confidential, proprietary communication without permission or authority.
 - 9.8.2 Personal use which can interfere with the Company's computing resources or cause irritation, inconvenience to the recipients or other Members.
 - 9.8.3 Mass mailers or chain initiation / forwarding i.e sending or forwarding of any non business email to more than 2 individual recipients or any group id outside the Company is prohibited.
 - 9.8.4 Sending emails in excess of the email size shall be prohibited.
 - 9.8.5 Use of another Member's email account without express written permission.
 - 9.8.6 Impersonating or concealing one's identity.
 - 9.8.7 Revealing password to any other person.
 - 9.8.8 Use of email id in online mail groups, blogs etc without permission of HOD.
 - 9.8.9 Sending messages or viewing content which is offensive, discriminatory, inflammatory or defamatory about individual, group or organization, race, gender, religion, national origin, attributes or sexual preferences.
 - 9.8.10 Viewing / Sending messages containing any obscene, indecent or porno graphic material.
 - 9.8.11 Use of services such as Dropbox, Yousendit or any other file sending software or cloud based storage for the purposes of business communications.

10. Policy For Internet Usage

- 10.1 Company provides for centralized internet facility to Members for official purpose
- 10.2 Company may impose reasonable restrictions in respect of timings, duration, sites etc in the best interests of the Members and Company.

10.3 Acceptable Use

- 10.3.1 Browsing sites or search engines for business related work and furthering the knowledge in areas of expertise
- 10.3.2 Limited use for internet banking
- 10.3.3 Limited personal use.

10.4 Unacceptable Use

- 10.4.1 Unauthorized access / entry into any third party or Company's Computer System
- 10.4.2 Activity resulting in disruption to third party or Company operations
- 10.4.3 Playing online games, viewing or transmitting sexually explicit content, hacking, gambling or any such activity which is illegal and prohibited under applicable law(s)
- 10.4.4 Downloading software without permission of the IT Committee.
If any software is required for better productivity or for any official purpose, then Member may send a written or email request to the IT helpdesk. The IT team will evaluate whether the required software is safe to install and if found safe, IT will install it. Such software will be added to the safe software list of IT so that software can be installed in future without need for evaluation process. This list will be reviewed by IT department every year or on receipt of any information that such software can be rendered unsafe.
- 10.4.5 Posting confidential, proprietary information either of Company or any third party on social networking sites, groups, blogs etc.
- 10.4.6 Viewing / Sending fraudulent or obscene or messages designed to inconvenience others.
- 10.4.7 Sending messages or viewing content which is offensive, discriminatory, inflammatory or defamatory about any person. This is in relation to race, religion, national origin, attributes or sexual preferences.

10.5 Internet Privacy

- 10.5.1 Usage of Internet via Company's computer Network is not confidential
- 10.5.2 All accesses to internet will be logged. These logs will be viewed by authorized IT personnel. These can also be shared with the concerned HOD or HR. Logs can also be shared with law enforcement authorities when called upon to do so.

Usage of internet via company's computer network is not confidential and will be logged. The logs can be shared with concerned HOD or HR or law enforcement authorities if required.

10.6 Blogging & Use of Social Networking Sites

- 10.6.1 All blogs except for official blogs should carry the following disclaimer "The views expressed are personal and do not reflect views of the author's Employer".
- 10.6.2 Members shall use appropriate language for such blogging / micro sites, social network platforms. Such language should not hurt any person, class of persons or society's sentiments.
- 10.5.3 Any official blogs can be posted after obtaining written or email authorisation of respective MD & CEO, Corporate Communications Dept. and Investor Relations Dept.

11. Dial-in Access ("VPN") Policy

- 11.1 Members can use VPN connections to gain access to the Company's computer network from the outside. VPN access should be strictly controlled, using one-time password authentication as far as practicable.
- 11.2 It is the responsibility of Member with VPN access privileges to ensure that a VPN connection is not used by any non-Member to gain access to the Company's information system. A Member who is granted VPN access privileges must remain constantly aware that VPN connection between his/her location and the Company is literal extension of the Company's computer network, and that they provide a potential path to the Company's information. Member must take every reasonable measure to protect Company assets.
- 11.3 Subject to clause 15, analog and non-GSM digital cellular phones cannot be used to connect to Company's Computer Network, as their signals can be readily scanned and / or hijacked by unauthorized individuals. Only GSM & CDMA standard digital cellular phones are considered secure enough for connection to Company's Computer Network.
- 11.4 Dial in access account activity shall be monitored, and if a VPN account is not used for a period of six months the account will expire and no longer function. If dial-in access is subsequently required, the Member may request a new account in the manner prescribed.

11.6 Acceptable Use

- 11.6.1 Members shall keep domain password confidential.
- 11.6.2 Members shall have installed antivirus & its latest updates onto their Computer before using VPN.
- 11.6.3 Member shall not access the Company's Computer Network over VPN unless the Device used by the Member to access contains latest anti-virus programme.
- 11.6.4 Members shall not download / save / store any data on devices other than those that are Company provided.

11.7 Unacceptable Use

- 11.7.1 Members shall not save passwords in the phone book of the dial-up adaptor.
- 11.7.3 Members shall be careful to log out from the Computer on completion of the work.



12. Protection Of Information



12.1 Virus Protection

12.1.1 Company provides for various Antivirus agents for protection of computer system; currently McAfee is installed in all the computer systems to protect the system from Virus, Trojans, Logic bombs or any such unwanted programs. A firewall is installed at the perimeter of HO & all data centres connected via internet to protect internal network from hackers.

12.1.2 Acceptable Use:

12.1.2.1 Members should ensure that his / her desktops or laptops are configured with the standard anti-virus or any other security software that is used within the Company. This also applies to company provided or financed mobile devices.

12.1.2.2 Members should scan floppies, CD-ROMs or any plug & play data storage drive for viruses if any before connecting them to the system in the network.

12.1.2.3 Members should report virus attacks if any, to the system administrator along with the necessary details like name of the virus, the action taken and the results thereon.

12.1.2.4 All software should be installed with help of IT Infrastructure team only.

12.1.3 Unacceptable Use:

12.1.3.1 Members should not attempt to modify the configuration of the anti-virus installed on their desktops or laptops.

12.1.3.2 Members should not bring Floppies, CDs or any plug & play data storage drives from unknown sources

12.1.3.3 Members should not download or install any shareware or freeware on the Company's Computer systems.

12.1.3.4 Members should not connect computer systems to the Company's computer network without latest updated Antivirus installed.

12.1.3.5 Members should not install any software on his / her own on the system.

12.2 Securing Data on Desktop/ Laptop Computers

12.2.1 All Computer Systems are pre-installed with backup agent for centralised data backup of Desktops / Laptop's onto the data backup server.

12.2.2 Acceptable Use:

12.2.2.1 Member's mail files, .pst files must be password protected and should be stored in email folder in the root of the drive.

12.2.2.2 Members should lock screen with passwords that activate after 3 minutes of inactivity. The screen should go blank after this period.

12.2.2.3 Members should keep their important data in a folder named "My data" or "My Documents" & .pst files in "Emails" folder in the root of the C or D drive.



12.2.2.4 Members should take back up of all important Data before travelling. If travel is for an extended duration i.e for more than 10 days, it is advisable to take a complete backup of the Data on to Computers

12.2.2.5 If Member's laptop Computer is lost, Member must immediately notify the nearest police station as well as the Company's Systems Manager, and give them specific information to identify their laptop Computer.

12.2.3 Unacceptable Use:

12.2.3.1 Members should not leave printouts of sensitive information unattended.

12.2.3.2 Members shall not share directories over the Computer Network without password protection and specific Member-level access;

12.2.3.3 Members shall not tamper with or attempt to modify the registry on Windows based systems.

12.2.3.4 Members should not leave laptops unattended in public places.

12.3 Clear Desk and Clear Screen Policy

12.3.1 Members are provided with a workstation having drawers with lock & key. External storage Devices are provided on request received from respective Member's HOD / Supervisor.

12.3.2 Acceptable Use:

12.3.2.1 Members shall take adequate precautions to protect the confidentiality and integrity of Confidential and Internal information that they deal with or that is made available to them.

12.3.2.2 Members shall protect files and other papers (non-electronic format) that contain sensitive or confidential information from unauthorized access.

12.3.2.3 If a confidential documents need to be printed, Members are advised to use password protected print outs. The SOP for the same is available on Mera Milaap.

12.3.2.4 Members shall ensure that unwanted printed paper containing confidential / sensitive information should be disposed off completely (Shredded), and all efforts should be made by Members to ensure confidentiality of the data being destroyed.

12.3.2.5 Members shall lock their workstation when idle.

12.3.2.6 When receiving sensitive faxes Members must be physically present to receive the same.

12.3.2.7 When transmitting sensitive faxes, Members are advised to inform the recipient of the fax first before transmission.

12.3.2.8 Members shall format the removable disk drives when the documents in it are not needed anymore.

12.3.3 Unacceptable Use:

12.3.3.1 Members should not leave any printouts unattended

12.3.3.2 Members shall not keep files & folders unattended.



12.4 Password Use

12.4.1 Passwords help in maintaining confidentiality of data and restricting access to authorized Members. Members are provided passwords to gain access to applications such as SAP, Email, Intranet and other applications.



12.4.1 Acceptable Use:

12.4.1.1 Members should use work group passwords solely within the Members of the group.

12.4.1.2 Members should keep passwords confidential.

12.4.1.3 Members should select and change their own passwords.

12.4.1.4 Members should change all Computer System-level passwords (e.g. root, enable, NT admin, application administration accounts, etc.) every month.

12.4.1.5 Members should change all Member-level passwords (e.g., email, web, desktop computer, etc.) at least every 45 days.

12.4.1.6 Members should conform passwords implemented on server level to the following:

12.4.1.6.1 The passwords should be at least 8 characters in length.

12.4.1.6.2 Password must include alphabets, numbers and must contain a special character.

12.4.1.6.3 Passwords must not contain dictionary words.

12.4.2 Unacceptable Use:

12.4.2.1 Members shall not use obvious and easily guessable passwords.

12.4.2.2 Members shall not store passwords on computer system in an unprotected form / clear text.

12.4.2.3 Members shall not reveal passwords to others.

12.5 Safe Disposal of information storage devices

12.5.1 Members should adhere to the following:

12.5.1.1 Be attentive when handling Device that will be disposed of.

12.5.1.2 For disposal of hard disk, pen drives, they must be formatted multiple times and low level formatting of hard disks must be ensured before disposal.

12.5.1.3 CD ROM and DVDs must be broken before disposal. Manual destruction or shredders may be used for the same if available.

12.5.2 Members shall not dispose external disk drives without following proper process as provided by the Company.

13.Laptop/desktop Usage Policy

13.1 Members shall maintain the integrity and prohibit misuse of device, computers, peripherals and other related resources that may be provided by the Company.

13.2 Acceptable Use:

- 13.2.1 Members shall consider the Computer and its related peripherals (mouse / monitor / keyboard / external storage Devices etc.) assigned for official purpose and should not swap with any Computer within or outside their departments.
- 13.2.2 Members shall maintain the identity of computers by not tampering with the asset ID and vendors Serial No. (E.g. Toshiba / IBM / HP etc). Member shall inform the IT department in the event of these labels not available on their machines.
- 13.2.3 It is recommended that temporary files on computers shall always be deleted on a regular basis as this utilizes a lot of disk space and can slow down the performance of the computer. Members must take help from IT support person for doing the same, if required.
- 13.2.4 Member must lock his desktop / laptop (Ctrl+Alt+Del+Enter) while leaving the desk for extended periods of time.
- 13.2.5 Important files must be encrypted / password protected and placed on separate disk partition other than partition on which the Operating System is installed.
- 13.2.6 Members are discouraged to share their folders as a normal practice. If at all it is required then the Members may share the folders in "READ only" mode and if required passwords protect them.
- 13.2.7 Guest Account on Computer Network must be disabled by default and Members shall not be enabling it under any circumstances.
- 13.2.8 Administrator account must be renamed and must have strong password as laid down by the password policies.
- 13.2.9 Screen savers with password shall be used to protect the machine from unauthorized access.

The Member should take good care of their assigned Devices.

13.3 Unacceptable Use:

- 13.3.1 Members shall not change the basic input output settings as configured by IT dept. on their computers.
- 13.3.2 Members shall not use objectionable wallpaper on the device provided to them by the Company.
- 13.3.3 Members shall not under any circumstances change the hostname or IP address of their Computers.
- 13.3.4 Members shall not use the "administrator" Member account for logging on to the Computer System.
- 13.3.5 Members should not tamper or dismantle their workstation, Desktops and Laptop Computer or any Devices attached with the computer systems.

13.3.6 Members should not attach any personal Devices with the computer like pen-drive, external HDD, CD writer, floppy drive or any other storage Device including iPods. In case Member wants to do it for some business purpose then it should be approved in writing by HOD / Head - IT.

13.3.7 Members should not allow visitors / guest to connect their laptop / any Device with the Company's Computer Network.

13.3.8 Members can connect only Devices which are provided by the Company for official purpose

14. Software Usage, Maintenance And Monitoring

14.1 Members shall ensure proper utilization of software used at the Company's Computer System and Computer Network and to control unapproved / unauthorized software usage.

14.2 Acceptable Use:

14.2.1 Members shall request for installation of new software by any employee must have an approval from his / her reporting manager and must have a valid license.

14.2.2 Members shall be aware that IT Committee reserves the right to seek justification from any Member for installation of any particular software and may suggest alternate software in best interest of the Company.

14.2.3 Members shall not install software on devices provided by the Company (like music players, chatting messengers etc.) Devices are handled by IT support and they must be informed if any changes are required to be carried out.

14.2.4 Members must ensure that antivirus patches and windows updates are applied on a regular basis (Once in every 15 days).

14.2.5 Members shall not override, disable or change configuration of Windows updates or antivirus updates.

14.2.6 Members shall disable the macros in case a file that is received contains macros that they are unsure about.

15. Wireless Communication Policy

15.1 This part of Policy prohibits access to the Company's Computer Networks via unsecured wireless Communication mechanisms.

15.2 This part of Policy is applicable to all wireless Communication Devices connected to any of the Company's Computer Network. This includes any form of wireless Communication Device capable of transmitting packet data. Wireless Devices and / or Networks without any connectivity to the Company's Network do not fall under the purview of this Policy.

Only wireless systems that meet the criteria of this Policy or have been granted an exclusive waiver by the IT department are approved for connectivity to the Company's Computer Networks.

15.2 Register Access Points And Cards

15.2.1 All wireless access points / base / stations connected to the Company's Computer Network must be registered and approved by the IT department. These access points / base stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards used in corporate laptop or desktop computers must be registered with the IT department.

15.3 Approved Technology

15.3.1 All wireless LAN access must use Company-approved vendor products and security configurations.

15.4 VPN Encryption And Authentication

15.4.1 All Computers with wireless LAN Devices must utilize a Company-approved VPN configured appropriately to prevent unauthorized access into the Company's Computer Network. To comply with this Policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e., MAC address. All implementations must support and employ strong Member authentication.

15.4.2 All gateways / routers acting as base stations / wireless hotspots should be configured to log all terminals connected to / through it and the logs should be stored for a minimum period of three months unless specified otherwise specified by any law for the time being in force.

15.4.3 Use of unsecured wifi such as those found in airports / coffee shops is allowed only if used along with VPN. This is because any hacker can eavesdrop and gain access to your computer



15.5 Setting The Service Set Identification (SSID)

15.5.1 The SSID should be configured so that it does not contain any identifying information about the organization, such as the Company name, division title, employee name, or product identifier.

15.5.2 The SSID key must use strong cryptographic controls and be set to WPA-PSK authentication at a minimum.

15.5.3 This facility will be configured and made available only by IT personnel and none other.

16. Due Diligence Measures

16.1 Members shall not view, create, host, display, upload, modify, publish, transmit, update or share any information that —

16.1.1 belongs to another person and to which the Member does not have any right

16.1.2 is harmful, harassing, blasphemous, defamatory

16.1.3 obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever

16.1.4 harms minors in any way

16.1.5 infringes any patent, trademark, copyright or other proprietary rights

16.1.6 violates any Applicable Law for the time being in force

16.1.7 Deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature

16.1.8 impersonates another person

16.1.9 contains software viruses or any other Computer code, files or programs designed to interrupt, destroy or limit the functionality of any Computer Resource;

16.1.10 threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation.

16.2 The Company shall remove any Information or Data specified in clause (2) above or Communication link to any such Information or Data within 36 (thirty-six) hours of such Information, Data or Communication link coming to the actual knowledge of the Company;

16.3 The Company may preserve such information as is specified in clause 2 above and associated records for at least 90 (ninety) days for investigation purposes;

16.4 The Company may appoint and keep appointed at all times a Grievance Officer to provide information or any assistance to Government agencies who are lawfully authorised for investigative and protective cyber security activity, on a request in writing stating clearly the purpose of seeking such Information or any such assistance.

16.5 At no time shall the Company knowingly deploy or install or modify the technical configuration of any Computer Resource or become party to any such act which may change or has the potential to change the normal course of operation of the Computer Resource than what it is supposed to perform, thereby circumventing any law for the time being in force, except where such technological means is developed, produced, distributed or employed for the sole purpose of performing the acts of securing the Computer Resource and Information contained therein.

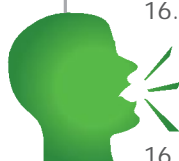
16.6 The name and contact details of the Members of IT Committee appointed under this Policy shall be published on the Company's corporate website.

16.7 The mechanism by which Members or any victim who suffers as a result of access or usage of IT Devices by any person in violation of clause 2 of these due diligence measures can notify their complaints against such access which may be made publicly available and published on the Company's corporate website.

16.8 IT Committee shall ensure that it will redress all complaints made under this Policy; within one month from the date of receipt of complaint.

17. Indemnity By Members

17.1 The Member shall hereby indemnify and agrees to keep indemnified Marico from or against any loss, damage, demand, claim, penalty, liability including but not limited to third party claims, that are lodged on the Company and that may arise statutorily or otherwise with regard to the breach, non-compliance, mal compliance, part compliance of the obligations of the Member as stated in this Policy.



18. Enforcement

Members are encouraged to report any improper activity.

18.1 Constitution of IT Committee:

18.1.1 A permanent committee comprising EVP & Head-Legal, Head-IT, EVP & Head-Global HR is constituted to enforce this Policy and it is also the redressal mechanism under this Policy. Such committee shall be known as "IT Committee". The Head-HR of the relevant company will be a special invitee to this committee. All decisions that the IT Committee are required to take under this Policy shall be taken unanimously.

18.1.2 All decisions of the IT Committee shall be final and binding.

18.1.3 IT Committee shall report to the MD & CEO.

18.2 Anonymity and Confidentiality

18.2.1 When a Member reports any grievance to the IT Committee through any medium, such Member may choose to remain anonymous, although Members are encouraged to identify himself / herself to facilitate communication and investigation.

18.2.2 If Member makes his / her identity known, the IT Committee and investigators will take every reasonable precaution to keep such Member's identity confidential.

18.3 Members have multiple options to reach IT Committee to report any grievances / post any query / concern. Member may choose to reach out to multiple Members in the Company who shall be equipped to help such Member resolve concern:

1. Line management
2. Line HR Manager
3. Any Member of the IT committee or Code of Conduct Committee.



18.4 Investigations

18.4.1 The procedures for handling potential violations of this Policy have been developed to ensure consistency in the process across the organization. Within this framework, Company will ensure it follows local grievance procedures, if any specified by the local laws.

18.4.2 While conducting an Investigation following any complaint, the Company will ensure it adheres to the Principles of natural justice namely:

18.4.2.1 Both parties shall be given reasonable opportunity to be heard along with witnesses and to produce any other relevant documents

18.4.2.2 No Person will be allowed to be a judge in his / her own case

18.4.2.3 The final decision will be made after due investigation and the application of proper reasoning

18.4.2.4 The order of the IT Committee shall be in writing and shall contain reasons for arriving at the decision

18.4.3 The decision of the IT Committee shall be published on the Company's corporate website.



18.5 Compliance

The Head-IT shall be responsible to submit a report of all incidents / grievances reported to the IT Committee every quarter to the MD & CEO and Compliance Officer of the company.

19. Penalty

19.1 Non-compliance or violation of this Policy will result in disciplinary action against the Member as may be decided by IT Committee and shall include termination.

19.2 The penalty for negligent non compliance of the Policy for the second instance will be reprimand which may be permanently noted in the personnel records of the relevant persons and additionally, the performance allowance and / or other allowances or incentives of the relevant persons may be temporarily / permanently withheld as per the sole discretion of the IT Committee.

19.3 The penalty for subsequent negligent non compliance of the Policy shall be termination from employment followed by arbitration proceedings to determine damages. The sole arbitrator shall be appointed by IT Committee.

19.4 In case of willful and deliberate non compliance of this Policy, the employment of the non-compliant Member or association of the non-compliant Member shall be liable to be terminated without any compensation.

19.5 Additionally, if no financial loss is caused by the willful and deliberate non compliance, a nominal penalty may be imposed at the sole discretion of IT Committee.

19.6 In case financial loss is caused by the willful and deliberate non compliance, then IT Committee shall determine damages if any.

19.7 It may be noted that none of the above preclude the Company from filing criminal complaints, before the appropriate legal authorities, against the persons who have negligently or deliberately breached the provisions of this Policy.

19.8 Notwithstanding anything contained above, the IT Committee will decide on the penalty commensurate with the gravity of the breach.

19.9 Notwithstanding anything stated herein, the Company may take legal action (Civil / criminal) against the Member for violation of this Policy or Applicable Law.



20. Severability

If any provision of this Policy is or becomes illegal, invalid or unenforceable, such provision shall be severed and the remaining provisions shall continue unaffected.

21. Amendment

This Policy can be amended by the Company at its discretion. The IT Committee shall notify any amendments to the policy on the Company intranet inviting comments and suggestions. The Company may after considering the comments and suggestions may make suitable further amendments. Such further amendments, if any, shall come into force immediately with effect from the date of such notification of the amendment.

22. Affirmation Of Acceptance And Acknowledgement:

Each Member should affirm acceptance of Marico's Information Security Policy through a declaration that should read as prescribed below:



I have received and read Marico's Information Systems Security Policy.

I understand the matters contained therein that there may be additional policies / guidelines or laws specific to my role.

I agree to comply with the Marico's Information Security Policies and Guidelines in spirit and letter.

I shall:

- a) keep myself abreast of the physical security and authentication rules in accessing the information systems authorized for use;
- b) adopt additional vigilant security practices while using mobile devices like (Laptops, Smart Phone, mobile phones etc);
- c) secure passwords and not share them;
- d) use the facility of the Company for the Company's business purposes only;
- e) restrict instant messaging only for the Company business purpose and not to send/receive text / audio / video file to any other person;
- f) use centralized file share facilities to store data where possible, and limit copies on local storage / removable media.
- g) not download and / or install any type of content / software / material either directly or indirectly through Company's IP address or otherwise onto Computer system without express permission or approval from IT Committee.

Signed_____

Name_____

Type of Association (tick which ever is appropriate)

Employee / Trainee / Associate / Consultant / Retainer / Contractor / Vendor / Supplier / Distributor / Apprentice

(if any other, specify): _____

Date_____

Appendix I

Systems Asset Requisition Form

Date of Request:	Name of the Member:s
Location:	Emp. No.:
Division/Department:	Floor/Block (if applicable):
Grade:	Extn No:
Requisition For:	
Purpose:	
Benefits:	
Name of HOD:	
Name of MD & CEO:	
Signature of the Member:	

** Above information will be used to prepare the CEP, if required.*

For System Use:	
Request received date:	
Request accepted / rejected:	
Please mention the alternatives explored to meet the Member request:	
Is the required asset available in working condition to meet the mentioned requirement?	
If not, what is the cost of the requested asset?	
Through what resource will the requested asset be procured?	
Date action initiated on:	Expected completion date:
CEP reference no., if any:	PO reference no., if any:
Name of the Authorizing Systems Person:	
Signature of Systems Person:	

Appendix II

Gate Pass Card for Issuing Portable Assets
(to be retained with security personnel)

G.P. Sl.

Name of the Member: Emp. No.:				Division/Department: Location:				
Machine Sl. No.: Adapter Sl. No.:				MIL Asset No.: Insurance Policy No.:				
Make: Model:				Configuration:				
Type of Asset (please tick): <input type="checkbox"/> Capital Item <input type="checkbox"/> Loan Item <input type="checkbox"/> Vendor Standby Item <input type="checkbox"/>								
Date of issue:				Authorized by (Name): Designation:				Date: Signature:
Date	Time Out	Receiver's Name & Signature	Security's Signature	Date	Time in	Depositor's Name & Signature	Security Signature	Remarks/Purpose of issue
<p>This item is the sole property of Marico Limited. This item is provided to me for the official use and I am fully accountable for any theft/damage/loss.</p> <p>Marico Limited has all rights to question me or recover money from me for the portable asset issued to me in the event of loss/theft/damage. I will return the company's asset issued to me at the time of transfer, separation or on demand. While I am in office I will keep the asset in lock and key if not in use.</p>								
Name of the Member & Signature:							Date :	

(to be retained by Administration Dept)

G.P. SI.

Name of the Member: Emp. No.:				Division/Department: Location:					
Machine SI. No.: Adapter SI. No.:				MIL Asset No.: Insurance Policy No.:					
Make: Model:				Configuration:					
Type of Asset (please tick): <input type="checkbox"/> Capital Item <input type="checkbox"/> Loan Item <input type="checkbox"/> Vendor Standby Item <input type="checkbox"/>									
Date of issue:				Authorized by (Name): Designation:				Date:	Signature:
Date	Time Out	Receiver's Name & Signature	Security's Signature	Date	Time in	Depositor's Name & Signature	Security Signature	Remarks/Purpose of issue	

Appendix III

Data Protection Policy

1. Introduction

Data Protection Policy for the Company ("DPP") sets out commitment of Marico to protect the privacy and integrity of sensitive personal data or information (defined later) collected by the Company.



2. Objective:

- 2.1 To ensure that data is collected and used fairly and lawfully
- 2.2 To process personal sensitive data or information only in order to meet its operational needs or fulfill legal requirements
- 2.3 To establish appropriate retention periods for personal sensitive data or information
- 2.4 To ensure that Members' rights can be appropriately exercised
- 2.5 To provide adequate security measures to protect personal sensitive data or information
- 2.6 To ensure that queries about data protection, internal and external to the organization, is dealt with effectively and promptly
- 2.7 To regularly reviewing data protection procedures and guidelines within the organization.

3. Applicability

- 3.1 The Company collects various information / data from its Members / associates ("provider of such information") which may be classified as:-
 - 1) Financial information
 - 2) Sensitive Personal information
 - 3) Physical health information
 - 4) Medical history
 - 5) Biometric information.
- 3.2 This information is requested by the Company at the time of joining / association. Further, personal information and sensitive personal information ("such information") / data are requested under a lawful contract.

4. Definitions

- 4.1 "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
- 4.2 "Information" includes data, text, images, sound, voice, codes, computer programmes, software and database or micro film or computer generated micro fiche;
- 4.3 "Personal information" means any information that related to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person;

4.4 "Sensitive personal data or information (SPDI)" of a person means such personal information which consists of information relating to:

- i) password;
- ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
- iii) physical, physiological and mental health condition;
- iv) sexual orientation;
- v) medical records and history;
- vi) Biometric information;
- vii) any detail relating to the above clauses as provided to body corporate for providing service; and
- viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the law relating to Right to Information or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

5. Purpose For Collecting Sensitive Personal Information

5.1 Marico collects sensitive personal information from its Members / associates for the purposes:

- 5.1.1 Biometric information is collected in order to provide uninterrupted ingress and egress in the Marico's premises
- 5.1.2 Financial information viz. PAN, Bank Account details, etc. are collected in order to direct credit any financial emolument to provider of such information
- 5.1.3 Medical history is collected in order to check the Health status.

6. Marico's Responsibility

- 6.1 Marico to obtain "Consent Form" [Appendix III (A)] from the provider of such information
- 6.2 Marico will not use / disseminate / disclose such information except for the purpose for which such information was collected. (To be read with point no.8)
- 6.3 Marico to provide privacy policy for handling of or dealing in such information including sensitive data or information;
- 6.4 Marico to request such information only under a lawful contract with the provider of such information and not otherwise;
- 6.5 However, Marico should not be held responsible pertaining to the authenticity of the personal information or sensitive personal information
- 6.6 Marico to ensure that such information is available for view by such provider of information who has provided such information under lawful contract
- 6.7 Marico shall publish such privacy policy on its website www.marico.com
- 6.8 Marico will provide access to such information to the provider of such information as and when request is received from the provider of such information.
- 6.9 Marico will keep such information secure as provided under the Applicable Laws
- 6.10 Marico will address any discrepancies and grievances of provider of such information with respect to processing of information in a time bound manner.
- 6.11 Marico has designated Head IT Infrastructure as Marico's "Grievance Officer".
- 6.12 Grievance Officer to redress such grievance within one month from the date of receipt of grievance.

7. Rights of Provider of such Information

- 7.1 Right to review - Provider of SPDI will have right to review such Information they had provide and ensure that any such information found to be inaccurate or deficient shall be corrected or amended as feasible.
- 7.2 Right to not to provide such information - Provider of SPDI shall be within his / her rights to deny providing of such Information to Marico, however, if such information is not provided then Company will be within its rights to deny any facility / service for which such information was sought.
- 7.3 Right to withdraw - Provider of SPDI will have an option to withdraw consent given earlier to Marico. Such withdrawal of consent to be sent in writing to Marico. Marico will be within its rights to deny any facility / service for which such information was sought.

8. Disclosure of such Information

- 8.1 Company will not use / disseminate / disclose such information except for the purpose for which such information was collected.
- 8.2 Company shall require permission from the provider of such information prior to disclosing such information to any third party.
- 8.3 Company will not require any prior permission from provider of such information when such information is to be shared / disclosed with Government / Governmental agencies mandated under law to obtain such information for the purpose of verification of identity or for prevention, detection, investigation including cyber incidents, prosecution and punishment of offences.
- 8.4 Notwithstanding anything contained in point 8.1 and 8.2 above, such information shall be disclosed to any third party by an order under the law for the time being in force
- 8.5 Company or any person in its behalf will not publish such information.

Appendix III (A)

Format of Consent Form

Personal / Sensitive Information Consent Form

Name of Member:

Employee Code:

Please Read Carefully, Complete and sign this form.

The Information Technology Act, 2000 and rules made there under mandates that consent be obtained prior to the collection and use of all personal / sensitive information.

The personal / sensitive information you provide to Marico will be used for the purposes reasonably associated with the employment / association.

“Sensitive personal data or information (SPDI) of a person means such personal information which consists of information relating to:

1. password;
2. financial information such as Bank account or credit card or debit card or other payment instrument details ;
3. physical, physiological and mental health condition;
4. sexual orientation;
5. medical records and history;
6. Biometric information;
7. any detail relating to the above clauses as provided to body corporate for providing service; and
8. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.”

Please specify from the above the type of personal / sensitive data or information that you are providing to the Company

These purposes include direct credit of salary, incentive amount / bonus, etc. and uninterrupted ingress / egress in the office premises by use of Biometric identification.

Additional personal information may be collected from time to time. Consent for the use of this personal / sensitive information may be inferred where its uses are obvious and it has been voluntarily provided.

Complete text of the Data Protection Policy for Marico (variously the “Policy” or “Policies”) may be found at www.marico.com

Should a Member wish to review their personal information held by Marico, they must make a request to the Marico pursuant to that Marico’s Policy.

Further, Member may withdraw consent to use their personal / sensitive information pursuant to the Policies. Such a withdrawal however, may require the cancellation of your employment/ association with and suspension of your activities with Marico.

All Members must sign a copy of this form.

I hereby consent to the receipt, collection, storage and use by the Company 39 all Sensitive Personal Data or Information that I have hitherto provided or May hereafter provide.

Signature of Member

Date:

MARICO INSIDER TRADING RULES, 2015

TABLE OF CONTENTS

Sr.No.	Contents	Page No.
1.	INTRODUCTION	3
2.	TITLE, COMMENCEMENT AND APPLICABILITY	4
3.	DEFINITIONS	5-9
4.	RESTRICTION ON COMMUNICATION AND TRADING BY INSIDERS 4.1. PROHIBITION ON COMMUNICATION OR PROCUREMENT OF UNPUBLISHED PRICE SENSITIVE INFORMATION 4.2. PROHIBITION ON TRADING WHILE IN POSSESSION OF UNPUBLISHED PRICE SENSITIVE INFORMATION 4.3. PROHIBITION ON TRADING DURING PROHIBITED PERIOD 4.4. MINIMUM HOLDING PERIOD 4.5. PRE CLEARANCE OF TRADES 4.6. DISCLOSURE AND REPORTING REQUIREMENTS	9-13
5.	TRADING PLANS	13
6.	COMPLIANCE OFFICER 6.1. DUTIES & POWERS OF COMPLIANCE OFFICER 6.2. ALTERNATE COMPLIANCE OFFICER	13
7	CODE OF FAIR DISCLOSURE AND CONDUCT 7.1. DISCLOSURE OF PRICE SENSITIVE INFORMATION 7.2. PROCEDURE FOR RESPONDING TO ANY QUERIES/REQUESTS FOR VERIFICATION OF MARKET RUMOURS BY STOCK EXCHANGES 7.3. DEALING WITH ANALYSTS/INSTITUTIONAL INVESTORS/MEDIA	14-15
8.	CHINESE WALL PROCEDURES	15
9.	'INSIDER SHARE TRADING' PORTAL ON MILAAP	15
10.	PENALTY FOR CONTRAVENTION 10.1. ACTION BY THE COMPANY 10.2. ACTION BY STATUTORY AUTHORITIES	16-17
APPENDIX I	FORM A - PART I FORMAT OF APPLICATION FOR PRE-CLEARANCE DURING FREE PERIOD FORM A - PART II FORMAT OF INTIMATION OF ACTUAL DEALING AFTER OBTAINING PRE-CLEARANCE FORM - B FORMAT OF INTIMATION FOR DEALING AT OR BELOW THRESHOLD LIMIT FORM - C - PART I STATEMENT OF IMMEDIATE RELATIVES & HOLDINGS IN THE SECURITIES OF THE COMPANY FORM - C - PART II ANNUAL STATEMENT OF IMMEDIATE RELATIVES AND HOLDING AND TRADING IN THE SECURITIES OF THE COMPANY FORM - D - APPROVAL FOR TRADING IN SECURITIES FORM - E - WAIVER OF MINIMUM HOLDING PERIOD FORM - F - REPORTING OF UNANTICIPATED PRICE SENSITIVE QUESTIONS RAISED DURING THE MEETINGS WITH THE MEDIA	18-19 20 21-22 23 24 25 26 27

1. INTRODUCTION

'*Insider Trading*' as understood under Indian law includes trading in the securities of the Company while in possession of unpublished price sensitive information and procurement or communication of unpublished price sensitive information, by Corporate Insiders such as Employees, Directors, their relatives and other persons connected with the Company.

Insider trading is not only unethical and immoral but also illegal as it fuels illegitimate speculation in the share prices on the Stock Exchanges. Such a profiteering by insiders by misusing confidential information available to them by virtue of their position or connection with the Company erodes investors' confidence in the integrity of the management of a company and adversely impacts the capital markets.

The Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015 ("SEBI Insider Regulations") which come into force on May 15, 2015 and the Companies Act, 2013 ("Act"), govern the law relating to insider trading in India. The SEBI Insider Regulations replace the erstwhile Securities and Exchange Board (Prohibition of Insider Trading) Regulations, 1992.

Accordingly, the Marico Insider Trading Rules, 2015 ("Rules") replace the erstwhile Marico Employees (Dealing in Securities & Prevention of Insider Trading) Rules of 2012, with effect from **May 15, 2015** to bring Marico's insider trading norms in line with the applicable law. The Rules have been approved by the Board of Directors of the Company at its meeting held on April 30, 2015 and further amended on April 29, 2016. Further, the Rules are embedded in Marico's Unified Code of Conduct.

It is clarified that these Rules are pursuant to and in furtherance, and not in derogation, of the laws applicable to insider trading in India. The text of the updated SEBI Insider Regulations is given in **Appendix II** to the Rules.

2. TITLE, COMMENCEMENT AND APPLICABILITY

- 2.1. These Rules shall be called "Marico Insider Trading Rules, 2015" or "the Rules".
- 2.2. These Rules are made pursuant to the Securities Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015, as amended from time to time (hereinafter referred to as 'SEBI Insider Regulations'/'the Regulations') and the Companies Act, 2013 and have been framed based on the Model Code specified in Schedule B to the Regulations without diluting the provisions of the Regulations in any manner.
- 2.3. The purpose of these Rules is to:
- 2.3.1. prohibit the communication of unpublished price sensitive information except for legitimate purposes, performance of duties or discharge of legal obligations;
 - 2.3.2. prohibit trading in the securities of the Company on the basis of unpublished price sensitive information;
 - 2.3.3. enable disclosure of trading by Insiders; and
 - 2.3.4. ensure appropriate, fair and timely disclosure of unpublished price sensitive information.
- 2.4. The Rules came into effect from May 15, 2015.
- 2.5. These Rules are mainly applicable to:
- 2.5.1. Insiders including Designated Persons (defined hereinafter); and
 - 2.5.2. Immediate Relatives of the persons stated in 2.5.1. above.
- 2.6. It is important to observe these Rules in its true spirit.

3. DEFINITIONS

3.1. Board of Directors or Board

Board means the collective body of Directors of the Company.

3.2. Chief Investor Relation officer

The Company has appointed the Chief Financial Officer as the Chief Investor Relation Officer of the Company for the purpose of these Rules.

3.3. Company

Company for the purpose of these Rules means Marico Limited.

3.4. Committee

Committee means the Audit Committee of the Board or such other Committee as may be nominated by the Board for the purpose of these Rules.

3.5. Compliance Officer

The Company has appointed the Company Secretary as the Compliance Officer for the purposes of the Rules and SEBI Insider Regulations, who shall work under the guidance of the MD & CEO and the CFO and report to the Board of Directors.

3.6. Designated Person(s)

Designated Person(s) mean:

- (i) All Promoters, Directors & Key Managerial Personnel;
- (ii) All employees in the Partner Grade;
- (iii) All employees in the following functions:
 - Corporate Accounts
 - Business Finance function
 - Treasury & Insurance
 - Corporate MIS
 - Corporate Taxation
 - Secretarial
 - Legal
 - Investor Relation
 - Strategy & M&A
 - Corporate Communications
- (iv) All Managers in the Finance, IT and the Business Process Transformation functions;
- (v) All Personal Secretaries/Executive Assistants, of the Director(s), Promoters and members of the Executive Committee, to the extent they are employees of the Company.
- (vi) Such other employees/persons as may be designated by the Board or the Committee or the Managing Director & Chief Executive Officer of the Company from time to time, to whom these trading restrictions shall be applicable, keeping in mind the objectives of these Rules.

3.7. Employee

Employee means an employee of Marico Limited and shall include any person deputed by Marico Limited to any subsidiary entity, trainees and temporary staff.

3.8. Executive Committee

Executive Committee shall mean the Committee designated as such by the Company.

3.9. Free Period

Free Period means any Period other than the Prohibited Period.

3.10. Generally Available Information

The term "Generally Available Information" means information that is accessible to the public on a non-discriminatory basis.

3.11. Immediate Relative

Immediate Relative means a spouse of a person, and includes parent, sibling, and child of such person or of the spouse, any of whom is either dependent financially on such person, or consults such person in taking decisions relating to trading in securities.

Note : It is hereby clarified that Spouse of a person will be considered immediate relative irrespective of whether he/she is financially dependent or consults such person in taking decisions relating to trading in securities.

3.12. Insider

Insider means any person who is:

- (i) a connected person ; or
- (ii) in possession of or having access to unpublished price sensitive information.

3.12.1. The term "**Connected Person**" referred in this definition of Insider means:

- (i) any person who is or has during the six (6) months prior to the concerned act been associated with the Company, directly or indirectly, in any capacity including the following that allows such person, directly or indirectly, access to unpublished price sensitive information or is reasonably expected to allow such access:
 - a. by reason of frequent communication with its officers; or
 - b. by being in any contractual, fiduciary or employment relationship; or
 - c. by being a director, officer or an employee of the company; or
 - d. holds any position including a professional or business relationship between himself and the company whether temporary or permanent.

3.12.2. Deemed to be a Connected Person

The persons falling within the following categories shall be deemed to be connected persons unless the contrary is established:

- a. an immediate relative of connected persons specified in clause 3.12.1; or
- b. a holding company or associate company or subsidiary company; or
- c. an intermediary as specified in section 12 of the Securities and Exchange Board of India Act, 1992 or an employee or director thereof; or
- d. an investment company, trustee company, asset management company or an employee or director thereof; or
- e. an official of a stock exchange or of clearing house or corporation; or
- f. a member of board of trustees of a mutual fund or a member of the board of directors of the asset management company of a mutual fund or is an employee thereof; or
- g. a member of the board of directors or an employee, of a public financial institution as defined in section 2 (72) of the Companies Act, 2013; or
- h. an official or an employee of a self-regulatory organization recognised or authorized by the Board; or

- i. a banker of the company; or
- j. a concern, firm, trust, Hindu undivided family, company or association of persons wherein a director of a company or his immediate relative or banker of the company, has more than ten per cent. of the holding or interest;

3.13. Key Managerial Personnel or KMP

Key Managerial Personnel or KMP means the following officers of the Company:

1. Managing Director & Chief Executive Officer;
2. Chief Financial Officer;
3. Company Secretary; and
4. Such other officer as may be appointed by the Company as a KMP from time to time.

3.14. Managing Director & Chief Executive Officer or MD & CEO

Managing Director & Chief Executive Officer or MD & CEO means the Managing Director and Chief Executive Officer appointed by the Company pursuant to the provisions of the Companies Act, 2013 read with Rules notified thereunder and designated as such by the Company.

3.15. Officer

Officer includes any director, manager or key managerial personnel or any person in accordance with whose directions or instructions the Board of Directors or any one or more of the directors is or are accustomed to act.

3.16. Prohibited Period

Prohibited Period shall mean the following:

a.	In respect of announcement of Quarterly/Half Yearly/ Yearly Financial Results by the Company	<ul style="list-style-type: none"> • Prohibited Period shall mean the period commencing from 1st day of the month immediately following the end of quarter/half year/year and ending 2 Trading days after the announcement of Financial Results for the respective quarter/half year/year, as the case may be, is made Generally Available by the Company. <p>ILLUSTRATION:</p> <p>For the quarter ended March 31, 2015:</p> <p>Date of commencement of Prohibited Period: April 1, 2015</p> <p>Date of conclusion of Prohibited Period: 2 Trading days after the Financial Results are made Generally Available by the Company.</p> <p>or</p> <ul style="list-style-type: none"> • Such other period as may be specified by the Compliance Officer from time to time after consultation with the MD & CEO or as may be directed by the Board or the Committee.
b.	In respect of Declaration of Dividends	<ul style="list-style-type: none"> • Prohibited Period will begin from such time as may be declared by the Compliance Officer after consultation with the MD & CEO or as directed by the Board or the Committee.
c.	In respect of change in capital structure	
d.	In respect of Mergers, de-mergers, acquisitions, delisting's, disposals and expansion of business and such other transactions	

e.	In respect of changes in key managerial personnel	
f.	In respect of material events in accordance with the listing agreement	
g.	In other cases	

• The Compliance Officer shall declare a prohibited period when he determines that a designated person or class of designated persons can reasonably be expected to have possession of unpublished price sensitive information. Such closure shall be imposed in relation to such securities to which such unpublished price sensitive information relates.

3.17. Promoter

Promoter means Promoter as defined under the Securities and Exchange Board of India (Issue of Capital and Disclosure Requirements) Regulations, 2009, as amended from time to time and shall include Promoter Group as defined therein.

3.18. Rules

Rules means the Marico Insider Trading Rules, 2015 as amended from time to time.

3.19. SEBI

SEBI means the Securities Exchange Board of India.

3.20. SEBI Act

SEBI Act means the Securities & Exchange Board of India Act, 1992

3.21. SEBI Insider Regulations

SEBI Insider Regulations means the Securities Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015, as amended from time to time.

3.22. SEBI LODR Regulations

SEBI LODR Regulations means the Securities Exchange Board of India (Listing Obligations and Requirements) Regulations, 2015.

3.23. Securities

Securities mean and include:

- (i) Equity shares of the Company;
- (ii) Such other marketable instruments as may be issued by the Company from time to time.

3.24. Subsidiary

Subsidiary shall have the same meaning as defined under section 2(87) of the Companies Act, 2013.

3.25. Trading day

Trading day means a day on which the recognized stock exchanges are open for trading;

3.26. Trading in Securities

Trading in securities means and includes:

- a) Subscribing, buying, selling, dealing or agreeing to subscribe, buy, sell or deal in any security of the Company and "trade" shall be construed accordingly;

- b) a gratuitous transfer of any securities of the Company;
- c) trading in the securities of the Company through a portfolio management account whether discretionary or otherwise and on the basis of investment advice rendered by any other investment advisor.

Note: the above sub-rule would not apply to dealing through Mutual Funds.

3.27. Unpublished Price Sensitive Information or UPSI

Unpublished Price Sensitive Information means any information, relating to the Company or its securities, directly or indirectly, that is not Generally Available which upon becoming Generally Available, is likely to materially affect the price of the securities and shall, ordinarily including but not restricted to, information relating to the following:-

- i. financial results;
- ii. dividends;
- iii. change in capital structure;
- iv. mergers, de-mergers, acquisitions, delistings, disposals and expansion of business and such other transactions;
- v. changes in key managerial personnel; and
- vi. material events in accordance with the SEBI LODR Regulations..

Words and expressions used and not defined in these Rules but defined in the "SEBI LODR Regulations", the SEBI Act, 1992 (15 of 1992), the Securities Contracts (Regulation) Act, 1956 (42 of 1956), the Depositories Act, 1996 (22 of 1996) or the Companies Act, 2013 (18 of 2013), and rules and regulations made thereunder, as amended from time to time, shall have the meanings respectively assigned to them in those legislations.

These Rules will be governed by the applicable laws and any provision(s), if not specifically provided herein, will operate as per the provisions of applicable laws.

4. RESTRICTION ON COMMUNICATION AND TRADING BY INSIDERS

4.1. PROHIBITION ON COMMUNICATION OR PROCUREMENT OF UNPUBLISHED PRICE SENSITIVE INFORMATION

- 4.1.1. No insider shall communicate, provide, or allow access to any UPSI, relating to the Company or its securities listed or proposed to be listed, to any person including other insiders except where such communication is in furtherance of legitimate purposes, performance of duties or discharge of legal obligations.
 - 4.1.1.1. Insiders should handle the UPSI with care and deal with the UPSI when transacting their business on a "need to know" basis.

"Need to know" basis would infer disclosure of UPSI only to those within the Company who need the information to discharge their duty and whose possession of such information will not, in any manner, give rise to a conflict of interest or likelihood of the misuse of the information.
- 4.1.2. No person shall procure from or cause the communication by any insider of UPSI, relating to the Company or its securities listed or proposed to be listed, except in furtherance of legitimate purposes, performance of duties or discharge of legal obligations.
 - 4.1.2.1. A person shall not procure UPSI unlawfully. Inducement and procurement of UPSI not in furtherance of one's legitimate duties and discharge of obligations would be illegal.
- 4.1.3. UPSI may be communicated, provided, allowed access to or procured, in connection with a transaction that would:-

-
- a. entail an obligation to make an open offer under the SEBI takeover regulations where the Board is of informed opinion that the proposed transaction is in the best interests of the Company;
 - b. not attract the obligation to make an open offer under the SEBI takeover regulations but where the Board is of informed opinion that the proposed transaction is in the best interests of the Company and the information that constitute UPSI is disseminated to be made Generally Available at least two (2) trading days prior to the proposed transaction being effected in such form as the Board may determine.
- 4.1.4. For purposes of clause 4.1.3., the Board shall require the parties to execute agreements to contract confidentiality and non-disclosure obligations on the part of such parties and such parties shall keep information so received confidential, except for the purpose of Clause 4.1.3., and shall not otherwise trade in securities of the company when in possession of UPSI.

4.2. PROHIBITION ON TRADING WHILE IN POSSESSION OF UNPUBLISHED PRICE SENSITIVE INFORMATION

- 4.2.1. No Insider shall trade in the securities of the Company listed or proposed to be listed when in possession of UPSI.

In the case of Connected Persons the onus of establishing, that they were not in possession of UPSI, shall be on such Connected Persons.

- 4.2.2. Trading in the securities of other companies

While discharging their role, employees may become aware of any unpublished price sensitive information relating to the Company's clients, suppliers or joint ventures. Such employees shall not deal in securities of such client, supplier or joint venture companies if they possess any unpublished price sensitive information in relation to that other company.

For example, if a person is aware that the Company is close to or is negotiating a significant/material investment or any corporate structuring transaction or an alliance with another company or any contract or transaction which qualifies to be unpublished price sensitive information, he should not deal in the securities of either Marico Limited or the other company.

4.3. PROHIBITION ON TRADING DURING PROHIBITED PERIOD

- 4.3.1. Designated Persons and employees (including their immediate relatives) shall not deal in the securities of the Company during the Prohibited Period including by way of exercise of stock option(s) or sale of shares allotted upon exercise of such stock options.

4.4. MINIMUM HOLDING PERIOD

- 4.4.1. Designated Persons (including their immediate relatives) who buy or sell securities shall not enter into an opposite transaction during the next 6 (six) months following the prior transaction ("Opposite Transaction"). However, the restriction on Opposite Transaction shall not apply to:

- a) the exercise of options granted under ESOP Scheme announced by the Company from time to time;
- b) the sale of shares acquired under ESOP Scheme, provided that the Designated Person is not in possession of UPSI at the time of such sale. However, once the shares acquired under the ESOP Scheme are sold by the person, any subsequent purchase (other than exercise of ESOPs) will be subject to the aforesaid restriction of Opposite Transaction.

- 4.4.2. In case the sale of securities is necessitated due to a personal emergency, the minimum holding period of 6 (six) months may be waived off by the Compliance Officer or MD & CEO or the Committee, after recording in writing the reasons in this regard and subject to the concerned person having obtained the approval of his Head of Department by making an application in **Form E** as annexed in the APPENDIX I to these Rules, provided such waiver does not violate SEBI Insider Regulations.

- 4.4.3. In case an Opposite Transaction is executed, inadvertently or otherwise, in violation of such a restriction, the profits from such trade shall be liable to be disgorged for remittance to SEBI for

credit to the Investor Protection and Education Fund administered by SEBI under the applicable law.

- 4.4.4. Designated Persons (including their immediate relatives) shall not take positions in derivative transactions in the securities of the Company at any time.
- 4.4.5. Designated Persons (including their immediate relatives) are strictly prohibited from entering into speculative transactions in the securities of the Company.

4.5. PRE CLEARANCE OF TRADES

- 4.5.1. Every Designated Person (including his immediate relative) who intends to trade in the securities of the Company, shall seek pre-clearance of transaction(s) before entering into such transaction(s) as per the pre-clearance procedure described hereafter, if the value of the securities traded, whether in one transaction or a series of transactions over any calendar quarter, aggregates to a traded value in excess of Rs. 10 Lacs.

Illustration:

Mr. X (Designated Person) holds 25,000 equity shares of the Company as at March 31, 2015. Mr. X now intends to sell 5,000 equity shares in three lots as under:

Lot 1 comprising 1,000 equity shares	During quarter ended June, 2015	Assuming Marico's Share Price was Rs. 380	Traded value of would be Rs. 3,80,000
Lot 2 comprising 2,000 equity shares	During quarter ended June, 2015	Assuming Marico's Share Price was Rs. 385	Traded value of would be Rs. 7,70,000
Lot 3 comprising balance 2,000 equity shares	During quarter ended September, 2015	Assuming Marico's Share Price was Rs. 390	Traded value of would be Rs. 7,80,000

Mr. X need not obtain pre-clearance for selling the first lot (as the traded value does not exceed Rs. 10 Lacs during a calendar quarter). However, before the sale of the second lot of 2,000 shares Mr. X shall pre-clear the transaction as the aggregate traded value of his dealings exceeds the threshold of Rs. 10 Lacs during a calendar quarter.

During the calendar quarter ended September, 2015, Mr. X may execute sale of 2,000 shares in lot 3 without requiring pre-clearance i.e. he can enter into fresh sale transaction(s) provided the traded value of such fresh transaction is upto Rs. 10 Lacs during that quarter, without seeking pre-clearance.

- 4.5.2. No Designated Person shall apply for pre-clearance of any proposed trade if such person is in possession of unpublished price sensitive information.
- 4.5.3. An application for pre-clearance of trades shall be made in **Form A- Part I** as annexed in the APPENDIX I to these Rules giving details of proposed trading(s).
- 4.5.4. The authority for pre-clearance of trades shall be as under:

Trading by following Designated Persons (including by their immediate relatives)	Authority for Pre-clearance
Directors/Promoters	The Committee
Members of Executive Committee	MD & CEO
Compliance Officer	MD & CEO
Other Designated Persons	Compliance Officer

- 4.5.5. The approval shall be granted within 2 trading days or such further time from the date of acknowledgement in **Form D** as annexed in the APPENDIX I to these Rules. In exceptional circumstances approval may not be given if there are reasons to believe that the proposed transaction is on the basis of possession of any unpublished price sensitive information. There shall be no obligation to give reasons for any withholding of approval.
- 4.5.6. Designated Persons who seek pre-clearance shall execute the trade(s) in respect of securities of the Company within 7 (seven) trading days from the date of the approval for pre-clearance or such shorter period as may be specified in the pre-clearance approval. If the transaction is not executed

within the time specified in the pre-clearance approval, the person shall pre-clear the transaction again.

- 4.5.7. Designated Persons who have dealt in securities of the Company after obtaining pre-clearance as aforesaid shall within 2 (two) trading days of such trading inform the actual details of their transaction(s) to the Compliance Officer in **Form A- Part II** as annexed in the APPENDIX I to these Rules.
- 4.5.8. Designated Persons (including their immediate relatives) trading in the securities of the Company below or at the threshold limit specified in para 4.5.1 shall within 2 (two) trading days of such trading inform the Compliance Officer details of the trading in **Form B** as annexed in the APPENDIX I to these Rules.
- 4.5.9. An undertaking accompanying the application in **Form A** or **Form B** shall be executed in favour of the Company by the Designated Persons incorporating the following statements:
- (a) the securities in respect of which approval is sought or intimation is provided, will be held/have been held by him/ her for a minimum period of six months (except for sale of shares acquired pursuant to ESOP Scheme);
 - (b) he/she does not have access to or has not received any unpublished price sensitive information upto the time of signing the undertaking;
 - (c) if he/she has access to or has received any unpublished price sensitive information after signing of the undertaking but before executing the transaction, he/she would inform the Compliance Officer of the change in his position and would completely refrain from trading in the securities of the Company till such time the information is made Generally Available;
 - (d) he/she has not contravened these Rules or the SEBI Insider Regulations, including any amendments thereto, as notified from time to time; and
 - (e) he/she has made a full and true disclosure required in the matter.

4.6. DISCLOSURE AND REPORTING REQUIREMENTS

4.6.1. INITIAL DISCLOSURE

- 4.6.1.1. Any person who becomes a Designated Person shall disclose to the Compliance Officer in **Form C-Part I** as annexed in the APPENDIX I to these Rules, details of himself and his immediate relatives, the number of securities of the Company held by him and his immediate relatives as on the date of becoming a Designated Person, within 7 (seven) trading days of his so becoming a Designated Person.

4.6.2. CONTINUAL DISCLOSURE

- 4.6.2.1. Every Designated Person shall be required to furnish to the Compliance Officer in **Form C-Part II** as annexed in the APPENDIX I to these Rules, for the following details, within 7 (seven) trading days after the close of the financial year:
- a. Details of his immediate relatives as on 31st March of the preceding financial year;
 - b. Details of trading in securities of the Company, by himself and his immediate relatives, during the preceding financial year; and
 - c. Details of securities of the Company held by him and his immediate relatives as on 31st March of the preceding financial year.
- 4.6.2.2. Every Designated Person and every employee of the Company shall disclose to the Company the number of such securities acquired or disposed of within two (2) trading days of such transaction if the value of the securities traded, whether in one transaction or a series of transactions over any calendar quarter, aggregates to a traded value in excess of Rupees 10 Lacs, in the format prescribed under the SEBI Insider Regulations.

For avoidance of doubt, it is clarified that the disclosure obligation under Clause 4.6.2.2. is in addition to the pre-clearance obligation set out in Clause 4.5.1.

4.6.3. DISCLOSURE BY OTHER CONNECTED PERSONS

The Compliance Officer may at his discretion require any other Connected Person or Deemed to be Connected Person to make disclosures of holdings and trading in securities of the Company in such form and at such frequency as he deems fit in order to monitor compliance with these Rules and SEBI Insider Regulations.

- 4.6.4. The disclosures to be made by any person under Clause 4.6 shall include those relating to trading by such person's immediate relatives, and by any other person for whom such person takes trading decisions.

5. TRADING PLANS

- 5.1. The SEBI Insider Regulations contain provisions enabling an Insider to formulate trading plan(s) and present it to the Compliance Officer pursuant to which trades may be carried out on his behalf in accordance with such plan. The provisions enable the formulation of a trading plan by an Insider to enable him to plan for trades to be executed in future.
- 5.2. The provision intends to give an option to persons who may be perpetually in possession of UPSI and enabling them to trade in securities in a compliant manner.
- 5.3. Insiders desiring to formulate Trading Plan(s) may do so in accordance with the provisions of the SEBI Insider Regulations.

6. COMPLIANCE OFFICER

- 6.1. In addition to the duties provided under the SEBI Insider Regulations and the Rules, the Compliance Officer shall have following duties/powers:
- 6.1.1. The Compliance Officer shall report to the Board and in particular to the Chairman of the Committee at such frequency as may be required by the Board.
- 6.1.2. The Compliance Officer shall promptly bring to the notice of the Share Trading Committee any instances of violation under the Rules.
- 6.1.3. The Compliance Officer shall place before the Committee an update on a quarterly basis capturing details of trading in the securities by Designated Persons and other employees/insiders of the Company.
- 6.1.4. The Compliance Officer shall maintain all records under these Rules and SEBI Insider Regulations for a minimum period of five (5) years.
- 6.1.5. The Compliance Officer shall notify the Stock Exchanges within two (2) trading days of any trading in the securities of the Company by any Promoter, Employee or Director in excess of the thresholds prescribed under clause 4.5.1
- 6.1.6. The Compliance Officer shall assist all employees in addressing any clarifications regarding SEBI Insider Regulations and these Rules.
- 6.1.7. The Compliance Officer shall ensure that prohibited period is intimated to all concerned at least 24 hours before the commencement of the said period.
- 6.1.8. The Compliance Officer shall promptly inform SEBI of any instances of violation of SEBI Insider Regulations after consultation with the Committee.

6.2. ALTERNATE COMPLIANCE OFFICER

- 6.2.1. During the temporary absence of the Compliance Officer, the Committee or the MD & CEO may appoint/ designate any other person to be an 'Alternate Compliance Officer' who shall act as the Compliance Officer for the purpose of these Rules and the SEBI Insider Regulations, during such temporary absence of the Compliance Officer.

7. CODE OF FAIR DISCLOSURE AND CONDUCT

7.1. DISCLOSURE OF PRICE SENSITIVE INFORMATION

- 7.1.1. Disclosure/dissemination of any UPSI shall be done promptly by, unless otherwise stated under the SEBI Insider Regulations, the Chief Investor Relations Officer and in his absence by the MD & CEO and in absence of both the aforesaid persons, by the Compliance Officer after consultation with the MD & CEO or the Chairman (hereinafter individually referred to as "Authorized Person"), by intimating to the Stock Exchanges and posting of the said information on the website of the Company and/ or otherwise making it Generally Available.
- 7.1.2. The Authorized Person shall, after disseminating any UPSI under clause 7.1.1., ensure uniform and universal dissemination / disclosure so as to avoid selective disclosure.
- 7.1.3. No UPSI shall be shared with any person unless the information is made Generally Available i.e. only public information can be shared.
- 7.1.4. In absence of the Authorized Person, such person as may be authorised by the MD & CEO, shall discharge the duties of Chief Investor Relations Officer as stated under Rules 7.1.1. to 7.1.3.

7.2. PROCEDURE FOR RESPONDING TO ANY QUERIES/REQUESTS FOR VERIFICATION OF MARKET RUMOURS BY STOCK EXCHANGES

- 7.2.2. The Authorized Person shall give an appropriate, fair and prompt response to the queries or requests for verification of market rumours by regulatory authorities.
- 7.2.3. As and when necessary, the Authorized Person shall make appropriate public announcement with respect to market rumours.
- 7.2.4. The Authorized Person shall make a prompt dissemination of UPSI that gets disclosed selectively, inadvertently or otherwise to make such information Generally Available.
- 7.2.5. In absence of the Authorized Person, such person as may be authorised by the MD & CEO, shall discharge the duties of Chief Investor Relations Officer as stated under Rules 7.2.1. to 7.2.4.

7.3. DEALING WITH ANALYSTS/INSTITUTIONAL INVESTORS/MEDIA

- 7.3.1. Only following persons are authorised to attend a meeting or interact with analysts/researchers, institutional and other investors or the media or any investor relations conference:
 - i) Any members of the Executive Committee
 - ii) Head – Investor Relation
 - iii) Manager – Investor Relation
 - iv) Head – Corporate Communication
 - v) Manager – Corporate Communication
 - vi) Any employee in the Partner Grade with the permission of any of the members of the Executive Committee
- 7.3.2. Any meeting or interaction with analysts/researchers, institutional and other large investors or the media or any investor relations conference shall be conducted in a manner that only information that is Generally Available is provided at such meetings/interactions.
- 7.3.3. Any such interaction/discussion may be preferably recorded through proceedings of the meeting or a transcript of the interaction with the analysts/researchers, institutional investors or other large investors or media or in any other suitable manner.
- 7.3.4. No UPSI shall be disclosed to Analysts/ Researchers or Institutional and other large investors unless prior confirmation from the Chief Investor Relations Officer and in his absence the Compliance Officer is obtained confirming that the said unpublished price sensitive information has been made Generally Available.
- 7.3.5. Alternatively, such information given to analysts/researchers etc. shall be simultaneously made Generally Available in consultation with the Authorized Person. If any UPSI is accidentally disclosed

without prior approval, the person responsible may inform the Authorized Person immediately of the same.

- 7.3.6. If unanticipated questions which are price sensitive are raised during the meeting, such questions shall be noted and a considered response shall be given only after consulting the Authorized Person. The concerned employee to whom the question has been posed, shall inform the Authorized Person in **Form F** annexed in the APPENDIX I to these Rules stating the queries and proposed response.
- 7.3.7. The Authorized Person shall issue a press release/transcript or post relevant information on the Company's website immediately after every analyst meet. Simultaneously, such information shall also be sent to the Stock Exchanges where any UPSI is disclosed. Alternatively, holding a live web casting of analysts meets may be considered.

8. CHINESE WALL PROCEDURES

- 8.1. All Designated Persons must maintain the confidentiality of all UPSI coming into their possession or control. To comply with this confidentiality obligation, the Designated Persons shall not:
- (ii) pass on any UPSI to any person directly or indirectly by way of making a recommendation for the purchase or sale of the securities of the Company; or
 - (iii) disclose UPSI to their family members, friends, business associates or any other individual, or
 - (iv) discuss UPSI in public places, or
 - (v) disclose UPSI to any Employee who does not need to know the information for discharging his or her duties, or
 - (vi) recommend to anyone that they may undertake trading in the securities of the Company while being in possession, control or knowledge of UPSI, or
 - (vii) be seen or perceived to be trading in the securities of the Company on the basis of UPSI.
- 8.2. Files containing UPSI shall be kept secure under lock and key. Computer files must have adequate security of login and password etc. All Designated Persons must follow the guidelines for maintenance of electronic records and systems as may be prescribed by the Compliance Officer from time-to-time in consultation with the person in charge of the information technology function. Each department shall nominate a member of the department who shall be responsible to ensure compliance with this clause.

9. 'INSIDER SHARE TRADING' PORTAL ON MILAAP

- 9.1. The text of these Rules, FAQs and SEBI Insider Regulations are available on the 'Insider Share Trading Portal' on Milaap.
- 9.2. Filing of Relevant forms prescribed under these Rules through Milaap:
- All forms prescribed under the Rules are available on 'Insider Share Trading' Portal on Milaap. All employees shall file the relevant forms mandatorily using 'Insider Trading Portal' on Milaap. Manual mode of filing shall be used by employees only in exceptional circumstances when it is not feasible to submit through Milaap. Approvals/ Rejections to be granted under these Rules by the concerned authority may be communicated either through Milaap or by email or in physical mode.
- 9.3. For any clarifications or queries, employees may log them on the portal at 'Insider Helpdesk' or contact the Compliance Officer directly.

10. PENALTY FOR CONTRAVENTION

10.1. ACTION BY THE COMPANY

- 10.1.1. An Insider who deals in securities in contravention of the provisions of these Rules, shall be guilty of insider trading.
- 10.1.2. Any violation under these Rules shall attract serious disciplinary action by the Company.

- 10.1.3. Persons who violate these Rules shall, in addition to any other penal action that may be taken by the Company pursuant to law, also be subject to disciplinary action including the termination of employment.
- 10.1.4. An Insider who violates the provisions of these Rules shall be liable to following penal/disciplinary actions:
- 10.1.5.

	Categories of Non-Compliances	Penal/ Disciplinary Actions
A]	Substantive Non-Compliances:	
1	Trading during Prohibited Period	An amount up to the higher of the following; i. two times the amount of gain made or loss avoided or ii. Rs.1,50,000 and / or Termination from Service
2	Trading on the basis of UPSI	
3	Undertaking Opposite transactions/ Derivative Transactions	
4	Making recommendation directly or indirectly on the basis of UPSI	
5	Communication / Passing on of UPSI	
6	Trading without seeking pre-clearance of trades	
B]	Procedural Non-Compliances:	
1	Non Reporting of transactions required to be reported post trading.	Warning Notice for the first instance of non-compliance. For every repeated act – a fine up to Rs. 25,000.

- 10.1.6. In addition to above penalties/action, the Insider who violates these Rules, shall be liable for such other disciplinary action by the Company which may include salary freeze, suspension, ineligibility for future participation in employee stock option plans, stock appreciation rights, etc.
- 10.1.7. The above actions of Company will be without prejudice to any civil or criminal action that the regulatory authorities may initiate against such defaulting Insider.
- 10.1.8. All cases of Substantive Non Compliances as defined in clause 10.1.4.(A) and Procedural Non-Compliances as defined in 10.1.4.(B) hereinabove involving any Insider, other than cases referred to in clause 10.1.10. hereinafter, shall be reported to and adjudicated by the "Share Trading Committee" ("STC") comprising the Chief Financial Officer, Chief Human Resource Officer, Compliance Officer/Alternate Compliance Officer and the Chief Legal Counsel..
- 10.1.9. STC may levy penalty within specified limits and it may take appropriate disciplinary/remedial action against the defaulting Insider and the decision of and the action taken by STC shall be final and binding upon the defaulting Insider.
- 10.1.10. STC shall, on a quarterly basis, submit a report on the action taken by it to the Committee which the Committee shall ratify. However, the Committee shall reserve the right to revise the penalty levied and/or action taken by STC and the decision of the Committee shall be final and binding on the defaulting Insider.
- 10.1.11. All cases of Substantive Non Compliances as defined in clause 10.1.4.(A) and Procedural Non-Compliances as defined in 10.1.4.(B) hereinabove involving following persons shall be reported to and adjudicated by the Committee which may levy penalty within the specified limits and/or take appropriate disciplinary / remedial action against the defaulting Insider and decision of the Committee shall be final and binding upon such person:
- Promoter
 - Director or KMP
 - Member of STC
 - Any member of the Executive Committee

10.2. ACTION BY STATUTORY AUTHORITIES

In the event of violation of the Companies Act or the SEBI Insider Trading Regulations, no penalty levied or other action taken by the Company will preclude SEBI or other appropriate authority(ies) from taking action under the relevant legislations.

Approved by: The Board of Directors of Marico Limited Original date of approval: April 30, 2015 Last Modified on: April 29, 2016 Effective Date: April 29, 2016
--

APPENDIX I

FORM – A
[Pursuant to Rule 4.5.1 to 4.5.3 and 4.5.9]PART I
FORM FOR APPLICATION FOR PRE-CLEARANCE OF TRADES

Date:

To: The Compliance Officer / MD & CEO/ Committee
Marico Limited (the "Company")

Dear Sir/ Madam,

I hereby give a notice pursuant to Marico Insider Trading Rules, 2015 (The "Rules") that I wish to trade in Securities of the Company as under: -

1. **Nature of Trade** *(please tick box)*Acquisition of Securities
Disposal of Securities 2. **Person executing the trade** *(please tick box)*Self HUF Immediate Relative *(specify name and relationship)* [Refer Rule 3.11]
_____Transaction done as Joint Holder _____
(specify First, Second or Third)3. **Details of Intended Trade (s):**

a) Date(s) of trade(s): _____

b) Number of Securities : _____

c) Class of Securities : *(please tick box)* Equity Preference Others _____

d) Name of the Depository Participant (DP) :

e) DP-ID/Client-ID / Folio Number:

f) PAN Number : _____

g) Type of Transaction : _____

(Open Market Purchase/ Open Market Sale/ ESOP Sale/ Off Market)

h) **Details of Securities held before execution of proposed trade(s) (including Joint Shareholding, if any)**

DP-ID/Client-ID/ Folio Number	Number of Securities

UNDERTAKING ACCOMPANYING FORM – A

In relation to the above trade(s), I undertake that:

- (a) The securities in respect of which the approval is sought, will be held/have been held by the above named for a minimum period of six months (except for sale of shares acquired pursuant to ESOP Scheme).
- (b) I am not and do not expect to be in possession of any Unpublished Price Sensitive Information at the time of the Trading.
- (c) In case, I receive any Unpublished Price Sensitive Information after signing this Form but before the execution of the trade, I shall inform the Compliance Officer of the change in the position and refrain from Trading in the securities till such information is made generally available.
- (d) I have not contravened the Rules or the SEBI (Prohibition of Insider Trading) Regulations, 2015.
- (e) I have made a full and true disclosure in the matter.
- (f) If approval is granted, I shall execute the trade within 7 trading days of the receipt of approval or such shorter period permitted in the approval, failing which I shall again seek pre-clearance.

Yours faithfully,

(_____)

Name:
Employee Code:
Designation:
Department:
Location:

APPENDIX I

FORM – A
[Pursuant to Rule 4.5.1 to 4.5.3 and 4.5.7]

PART II
FORM FOR INTIMATION OF ACTUAL TRADING AFTER OBTAINING PRE-CLEARANCE
 [To be submitted within 2 trading days of trading in Securities of the Company]

Date:

To:
 The Compliance Officer / MD & CEO/ Committee
 Marico Limited (the "Company")

Dear Sir/ Madam,

I hereby give intimation pursuant to the Marico Insider Trading Rules, 2015 (The "Rules") that I have executed following trade after obtaining pre-clearance from the Compliance Officer / Committee / CFO / MD & CEO:

1. **Nature of Trading** (please tick box)

Acquisition of Securities
 Disposal of Securities

2. **Person executing the Trade** (please tick box)

Self
 HUF
 Immediate Relative (*specify name and relationship*) [Refer Rule3.11]

 Transaction done as Joint Holder _____
 (specify First, Second or Third)

3. **Date of Pre-clearance** : _____4. **Details of Actual Trade(s):**

- a) Date(s) of Trade(s): _____
 b) Number of Securities : _____
 c) Class of Securities : (*please tick box*) Equity Preference Others _____
 d) Name of the Depository Participant (DP) : _____
 e) DP-ID/Client-ID / Folio Number : _____
 f) Details of Securities held after the aforesaid trade(s) (including Joint Shareholding, if any) :

DP-ID/ Client-ID/ Folio Number	Number of Securities

Yours faithfully,
 (_____)

Name:
Employee Code:
Designation
Department:
Location:

APPENDIX I

FORM – B
[Pursuant to Rule 4.5.8 and 4.5.9]

FORM FOR INTIMATION OF TRADING AT OR BELOW THRESHOLD LIMIT
 [To be submitted within 2 trading days of trading in Securities of the Company]

Date:

To: The Compliance Officer / MD & CEO/ Committee
 Marico Limited (the "Company")

Dear Sir/ Madam,

I hereby give a notice pursuant to the Marico Insider Trading Rules, 2015 (The "Rules") that I have executed the following trade in relation to securities of the Company (not being more than in number and value as prescribed in Rule 4.5.1. of the Rules): -

1. **Nature of Trading** (please tick box)

Acquisition of Securities
 Disposal of Securities

2. **Person executing the Trade** (please tick box)

Self
 HUF
 Immediate Relative (specify name and relationship) [Refer Rule 3.11]

Transaction done as Joint Holder _____
 (specify First, Second or Third)

3. **Details of Actual Trade(s):**

- a) Date(s) of Trade(s): _____
 b) Number of Securities : _____
 c) Class of Securities : (please tick box) Equity Preference Others _____
 d) Name of the Depository Participant (DP) : _____
 e) DP-ID/Client-ID / Folio Number : _____
 f) **Details of Transaction (Including Transaction done as Joint Holder, if any)**

DP-ID/Client-ID/ Folio Number	Number of Securities Pre-Trade	Number of Securities Post-Trade	Class of Securities

Yours faithfully,
 (_____)

Name:
Employee Code:
Designation
Department:
Location:

FORM – B
[Pursuant to Rule 4.5.8 and 4.5.9]

FORM FOR INTIMATION OF TRADING AT OR BELOW THRESHOLD LIMIT
[To be submitted within 7 trading days from the date of trading in Securities of the Company]

UNDERTAKING ACCOMPANYING FORM – B

In relation to the above trade, I hereby undertake that

- (a) The securities in respect of which the aforesaid trading has been entered into, will be held/ have been held by the above named for a minimum period of six months (except for sale of shares acquired pursuant to ESOP Scheme).
- (b) I was not in possession of any Unpublished Price Sensitive Information at the time of the Trading.
- (c) I have not contravened the Rules or the SEBI (Prohibition of Insider Trading) Regulations, 2015.
- (d) I have made a full and true disclosure in the matter.

Yours faithfully,

(_____)

Name:

Employee Code:

Designation

Department:

Location:

APPENDIX I

FORM – C
[Pursuant to Rule 4.6.1.1]

PART I

STATEMENT OF IMMEDIATE RELATIVES & HOLDINGS IN THE SECURITIES OF THE COMPANY

(To be submitted within 7 trading days from becoming a Designated Person)

Date:

To: The Compliance Officer / MD & CEO/ Committee
Marico Limited (the "Company")

Dear Sir/ Madam,

Consequent to becoming a Designated Person (DP) of the Company, I hereby furnish the following details in terms of the Marico Insider Trading Rules, 2015 (The "Rules"):

1. Details of Designated Person

- a. Name : _____
- b. Designation : _____
- c. Function : _____
- d. Employee Code : _____
- e. PAN : _____
- f. Date of assuming office of Director / Officer/ DE : _____

2. Details of Immediate Relatives [as defined in Rule 3.11. of the Rules]

Name	Relation	PAN

3. Details of securities of the Company held by me and by my immediate relatives as on date of becoming DP:

Self / HUF/ Immediate Relative (Name)	DP-ID/ Client-ID / Folio No.	No. of Securities held	Class of Securities (Equity/Preferenc e, etc.)	If held in Joint Name (Specify First/Second/ Third)	Mode of acquisition (market purchase/ public/rights/ Preferential offer etc.)

Yours faithfully,

(_____)

Name:

Employee Code:

Designation:

Department:

Location:

APPENDIX I

FORM – C
[Pursuant to Rule 4.6.2.1]

PART II

ANNUAL STATEMENT OF IMMEDIATE RELATIVES AND DETAILS OF THE SECURITIES OF THE COMPANY*(To be submitted within 7 trading days from the end of the financial year)*

I hereby furnish the following details pursuant to Marico Insider Trading Rules, 2015 (The "Rules"):

1. Statement of Immediate Relatives and details of securities held as on 31st March _____ *(previous Financial Year ending)*

Full names and Demat details of Immediate Relatives [as defined in Rule 3.11. of the Rules]

Sl. No.	Name	Relationship	PAN	DP-ID/ Client-ID / Folio Number	No. of Securities held	Class of Securities

2. Details of Trading in Securities of the Company during the Financial Year ending March 31st

Sl. No.	Self / HUF/ Immediate Relatives (Name)	Date of Trading	No. of Securities			Class of Securities
			Purchased	Sold	Balance	

I declare that above details are true, correct and complete in all respects.

Yours faithfully,

(_____)

Name:
Employee Code:
Designation
Department:
Location:

APPENDIX I**FORM – D**
[Pursuant to Rule 4.5.5]**APPROVAL**

Date:

From:

The Compliance Officer / MD & CEO/ Committee
Marico Limited (the "Company")
Mumbai

To: _____

Dear Sir/Madam,

Your application dated _____, seeking approval to deal in _____ securities of the Company is hereby acknowledged. Having regard to the information furnished, consent is as under: (see ticked box)

GIVEN**REFUSED****GIVEN ON THE FOLLOWING CONDITIONS**

- (a) You are not and do not expect to be in possession of any Unpublished Price Sensitive Information at the time of the Trading.
- (b) You have not contravened the Rules or the SEBI (Prohibition of Insider Trading), Regulations, 2015 (SEBI Insider Regulations).
- (c) You have made full and true disclosure in the matter.

Note 1: Designated Persons who trade in manner (i.e. buy/ sell or otherwise deal) in the securities of the Company shall not enter into an opposite transaction i.e. buy / sell/ or otherwise deal in securities of the Company during the next six months following the prior transaction."

Exception:

An employee can exercise his ESOPs even if he has transacted in shares of the Company during the previous six months. However, once the shares acquired under the ESOP Scheme are sold in the market, the restriction on buying would become applicable for next six months.

Thus, after the current sale transaction, you may continue to sell shares in the market, but will not be allowed to buy for the next six months from the date of your latest sale & vice versa.

Note 2: In case you have received any "Unpublished Price Sensitive Information" after submission of your application for sale of securities, please inform the Compliance Officer of the change in the position and refrain from trading in the securities till such information is made generally available.

Note 3: This approval has been granted for trading in securities within _____ trading days w.e.f. _____ failing which please seek pre-clearance again.

Yours faithfully,
(Compliance Officer / MD & CEO/ Committee)

APPENDIX I

FORM – E

WAIVER OF MINIMUM HOLDING PERIOD
[Pursuant to Rule 4.4.2]

Date:

To: The Compliance Officer / MD & CEO/ Committee
 Marico Limited (the "Company")

Dear Sir/ Madam,

I request you to grant me a waiver of the minimum holding period of six months as required under the Marico Insider Trading Rules, 2015 with respect to _____ securities of the Company held by me/ my Immediate Relatives/ HUF _____ (Name) singly/ jointly acquired by me / my Immediate Relatives/ HUF on _____ (Date).

I desire to deal in the securities on account of following (give reasons and supporting documents).

--

I declare that:

- a) The above details are true, correct and complete in all respect; and
- b) I am not and do not expect to be in possession of any Unpublished Price Sensitive Information at the time of the Trading.
- c) The trade if made shall not be in contravention of the SEBI (Prohibition of Insider Trading) Regulations, 2015.

Thanking you,

Yours faithfully,

(_____)

Name:**Employee Code:****Designation****Department:****Location:**

APPROVAL OF HOD APPROVED NOT APPROVED

(for office use only)

APPROVED

REJECTED

(The Compliance Officer / MD & CEO/ Committee)

APPENDIX I

FORM – F
[Pursuant to Rule 7.3.5 and Rule 7.3.6]

Date & Time of Meet: _____ Type: Analyst Media/PR Others _____
(Please specify)

Venue: _____
Purpose: _____

Name/s of Analyst(s) / Media / PR: 1. _____
2. _____
3. _____

Persons to be present: 1. _____
(From the Company) 2. _____
3. _____

Nature of Information: The following information pertaining to unpublished price sensitive information as specified in clause 3.26 of the Rules is being sought:

Sr. No.	Category	Details of Unpublished Price Sensitive Information

Approved by : _____
(Authorized Officer)

Yours faithfully,
(_____)

Name:
Employee Code:
Designation
Department:
Location:

Note:

“Unpublished Price Sensitive Information” means any information, relating to the Company or its securities directly or indirectly, that is not generally available and which upon becoming generally available, materially affect the prices of securities of the Company.



Marico's Code of Conduct (CoC)



ACKNOWLEDGMENT / CONSENT FORM



ACKNOWLEDGMENT / CONSENT FORM

Affirmation of acceptance and acknowledgement:

Each Member shall affirm acceptance of this Code through declaration that shall read as prescribed below:

For new Joinees:

I have received and read Marico's Unified Code of Conduct for Members with its Annexures. I understand the matters contained in the Code and understand that there may be additional policies or laws specific to my role. I agree to comply with the Code in spirit and letter.

Signed _____

Name _____

Date _____

Quarterly Affirmation

I have complied with this Code during the Quarter _____

Signed _____

Name _____

Date _____

Marico Ltd.

Phone: 022-6648-0500

For feedback, queries, suggestions, please write to speakupmarico@ethicshelpline.in

©Marico Limited 2014

