ASSET ISSUANCE
&
ACCEPTABLE USAGE POLICY

Prepared by:	Reviewed by:	Approved by:
Mohammed Waseem	**AbdulRazaq AlDaham**	
Sr. Project Administration	Manager – HR and Admin	

Office No. 503, Noura Tower, P.O. Box. 34412, Prince Turki Road, Al Kurnaish Dist., Al Khobar, Saudi Arabia
www.masco.com.sa

Contents

Introduction

The purpose of this policy is to establish guidelines for acceptable and unacceptable use of all information assets, electronic devices (laptops, mobiles phones, pen drives etc.) and network resources at designated work locations owned or in operation by MASCO GC in addition to its other established information security policies and procedures.

Scope

All Staff, contractors, consultants, temporary and other third-party contractors at or outside the designated work locations, including all personnel affiliated with client/third parties must adhere to this policy. This policy applies to information assets owned by the MASCO GC, or to devices that connect to its network or in usage by any authorized personnel for business purposes.

Objective

MASCO GC provides information assets, electronic devices and other network resources to the users to meet its objectives, goals and initiatives whereas the users are responsible to manage/maintain the confidentiality, integrity and protects its assets from damages of any nature.

Policy

Moral Obligations

- All the aforementioned users are expected to exercise and demonstrate ethical usage of MASGO GC's resources in conjunction with its standard guidelines. Usage of resources provided shall be solely for business purposes and any personal/unlawful is strictly prohibited unless any limited personal usage is agreed upon.
- Devices that seem to have compromised in terms of security should be immediately turned off and returned to the responsible IT/Administration staff.
- Allocated devices are advised to be turned off when not in use.

Individual Responsibilities

- It is the sole responsibility of the user to protect the assets (laptops, mobile phones, pen drives), accounts and informational access under their control/ownership. This responsibility also extends to the usage of designated software for business purposes.

- Usage of mobile phones shall be restricted to business purposes only unless otherwise specified usage is agreed upon.
- Passwords selected and adopted should adhere to the password standards policy. Sharing of passwords with anyone is a strict no-no.
- Information leakage or security breach of any kind either by system failure or deliberately disclosing it to an unauthorized person is a violation and shall be dealt in accordance to relevant policies.
- Users are advised to understand that the propriety information by any means (whether legal or by technical) always remains in control of MASCO GC.
- During the course of business, storing proprietary information on personal, third-party controlled medium or non-MASCO GC operated environment is strictly prohibited.

Security and Handling

- Information Assets provided should always be password protected.
- Electronic devices such as Laptop or any other asset (pen drives) should be properly locked in a drawer or cabinet by its owner while leaving the work place.
- All electronic devices (PCs, Laptops, Tablets etc.) should be secured with a password and if left unattended should be set to an automatic screen lock which activates within 5 minutes or even lesser.
- Users are advised not to bring their own laptops or other gadgets at workplace unless otherwise agreed for specific usage.
- Users own electronic devices or gadgets (if allowed) should not compromise the security of other information assets that are controlled by MASCO GC.
- Users are advised not to tamper or exercise any action that may result in distorting configurational settings with reference to firewall, antivirus or servers assigned to them.
- Usage of printers, scanners or the assigned storage medium (USB) should be for official purpose only.
- Usage of official email ID for personal benefits and vice versa is strictly prohibited.
- Circulating unofficial/spam/phishing emails to an individual or to a group of individuals is against the policy.
- Downloading unofficial content causing a disruption in the network is unacceptable and unethical.

Returning the Assets

- Users are advised to return the assets including all the electronic devices, mobiles phones, access to information (such as online business accounts, software, network folders etc.) under their ownership at the time of termination, resignation or if requested by the company.

Audit

- In an effort to adhere/execute regulatory requirements of MASCO GC, Governmental Standards or any other requirements stipulated by clients (Saudi Aramco, SABIC, SEC and other esteemed clients) and their effectiveness, authorized IT/Administration staff may audit info. systems and electronic devices that are provided to the users or to those who access its network. Users are requested to cooperate and do not interpret the audit as an offensive action against them.

Reporting

- Upon discovering security breach, theft or have lost the asset(s) provided by the company, the owner should immediately inform the designated IT/Administration staff copying his/her Reporting Manager and the IT/Administration Manager.
- Upon Termination, Resignation of MASCO GC staff or its affiliates assigned to locations/projects controlled by Saudi Aramco, SABIC, SEC and other listed clients. MASCO GC's authorized IT/Administration Staff will immediately inform the aforementioned clients and for dismissal/revoking access(s) assigned to the separating staff.

Implementation

- Users of company property, proprietary information will be subjected to strict disciplinary action up to and including termination if found violating this policy guidelines.
- Third Party/Contractual/Client Staff indulging in activities resulting in this policy violations may trigger an immediate withdrawal of their access to company properties and work locations.

Asset Issuance and Acceptable Usage Declaration

- Asset Issuance and Acceptable usage declaration form can be found on next page.