SIGMA ELECTRIC MANUFACTURING CORPORATION PVT LTD.
ACCEPTABLE USE POLICY

PURPOSE:
The purpose of this policy is to outline the acceptable use of electronic resources including computers, networks, electronic mail services and electronic information sources that are owned by or leased at SIGMA Electric Private Limited ("**SIGMA**" and / or "**Company**"). These rules are in place to protect both SIGMA's employees and the Company.

Inappropriate use of such resources exposes the Company to risks including virus attacks, compromise of network systems / services, and legal issues etc. This policy is committed to protecting the Company's employees, partners and the Company itself from illegal or damaging actions by individuals, whether committed knowingly, unknowingly, intentionally or unintentionally.

The intention of this Policy on Acceptable Use is not to impose restrictions that are contrary to the established culture of openness, trust, and integrity at SIGMA.

SCOPE:
This policy applies to SIGMA's employees (both permanent and temporary), contractors, consultants and employees of group companies, partners, and other workers at the Company, including all personnel affiliated with third parties ("Users") who use / can use electronic resources at SIGMA including computers, networks, electronic mail services and electronic information sources that are owned or leased by the Company ("Resources").

POLICY:
The Company recommends that any information that Users consider sensitive or vulnerable be encrypted.

For security and network maintenance purposes, authorized individuals within the Company may monitor Resources including equipment, systems, and network traffic at any time without any prior notice.

The Company reserves the right to audit Resources on a periodic basis & implement all appropriate action based on the findings of the audits.

All Users should keep passwords secure and do not share accounts. Authorized Users are responsible for the security of their passwords and accounts. Passwords should be changed at least once every three months and the system will prompt you to do so.

All PCs, laptops and workstations should be secured with a password protected screensaver with the automatic activation feature set at 10 minutes or less, or by

logging-off the computer (by pressing the Control+Alt+Delete keys and clicking on lock computer for Win2K and WinXP users).

All hosts used by Users that are connected to the SIGMA Internet/Intranet/Extranet or any other similar systems, whether owned by the User or SIGMA, shall be required to continually run approved virus-scanning software with a current virus database (unless overridden by departmental or group policy approved by SIGMA in writing).

Under no circumstances is a User of Resources at SIGMA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing systems owned or leased by SIGMA.

Employees should use internet services in a safe and responsible manner in accordance with all applicable IT and HR policies of SIGMA and otherwise in compliance with all applicable laws.

Users are prohibited from interfering with, disrupting or engaging in unauthorized use of SIGMA's Resources.

Notwithstanding the generality of the foregoing, Users shall, at all times, ensure that:

- Users do not use SIGMA's Resources for private business or commercial activities;
- Users do not engage in unauthorized use of SIGMA's name or any other use which is not connected with the operations or business of SIGMA;
- Users shall not use SIGMA's Resources to transmit, distribute or store material that is inappropriate / obscene / defamatory / libelous / threatening / abusive / violent or hateful. Users are prohibited from using SIGMA's Resources to view, store, or transmit pornographic and / or discriminatory material.
- Users shall not use SIGMA's Resources to transmit or distribute material containing fraudulent offers / promises for goods or services or any advertisement / promotional material that contains false, deceptive or misleading statements, claims or representations relating to SIGMA or any of its employees.
- Users shall not use any Resources to transmit or distribute or store material that may be harmful to or has the potential to interfere with SIGMA's or a third party's networks, systems, services, or websites. Prohibited or harmful content includes but is not limited to viruses, worms, password cracking programs or Trojan Horses.
- Users shall not access, possess distribute or retain confidential electronic information either belonging to SIGMA or a third party unless they are authorized to do so. Confidential information for purposes of this clause includes but is not limited to client lists, forecasts, sales figures, etc.
- Users shall not use or even attempt to use the computer accounts of others;

- Users shall not engage in any activity that may lead to misrepresentation of the identity of a person including the sender of an email etc. Further, deletion / alteration of the content of an electronic message originating from another person or computer with the intent to deceive, intercept or attempt to intercept a communication is strictly prohibited.

Violation of this policy will lead to disciplinary action as provided by the relevant law. This policy is an integral part of the employment service conditions. SIGMA reserves the right to modify or amend this policy at any time as it may deem necessary.

Should you have any questions in relation to this policy, please contact company Compliance Officer or Head, IT at your location.

AUPv.2
August 2013