INFORMATION SECURITY POLICY

Introduction

We have introduced the physical controls at server room by not permitting any unauthorized entry physically.

No visitor is allowed in this area without prior approval and they are not allowed to carry any laptops, pen drives, floppies, cds etc., inside the secured areas.

All employees are not allowed to carry any information in any form from the office while leaving the office. No direct access to Internet is provided to anyone other than authorized persons. All the computers are controlled, their activities are frequently viewed by senior officials time and again to ensure that no pilferage of any sensitive information.

No third party vendors, contractors are permitted in restricted zone. Any meetings with this person if required are held at non secured zone office at the front office.

Physical controls of office premises and facilities:

Physical security guard stationed at the entry point guards the office and no unauthorized entry is permitted. Apart from that Biometric locking arrangements are maintained.

Protecting against external environmental risks: No open or vacant area is left in the office.

Photographic video, audio or any recording equipments like cameras in mobile devices are not permitted inside the secured area. Even employees are not allowed to carry their mobile phones with camera to have full proof physical security of sensitive information.

We have also ensured to discard all unused or unserviceable equipments, Records, papers not required are destroyed to avoid the unnecessary piling up of unused materials to avoid the dust, fire, explosion, vibration, chemical, electrical damage.

Information Security policy and Network Security Policy Purpose

The purpose of this policy is to outline acceptable use of computer equipment at Company. These rules are in place to protect the entire Company's team and Company. In appropriate use expose risks including virus attack, compromise of network system and service and legal issues.

Scope

This policy covers employees, contractors, consultants and temporaries including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company.

Policy

1. The legitimate use of network and reasonable level of privacy is ensured.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

3. This policy recommends that any information that is considered sensitive is encrypted.

4. Regular Audit of network system is done on periodic basis to ensure the Compliance of this policy.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing company's owned resources.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

We have introduced the physical controls at server room, back office room by not permitting any unauthorized entry physically.

No visitor is allowed in this area without prior approval and they are not allowed to carry any laptops, pen drives, floppies, cds, etc. inside the secured areas.

All employees are not allowed to carry any information in any form from the office while leaving the office. No direct access to Internet is provided to anyone other than authorized persons. All the computers are controlled, their activities are frequently viewed by senior officials time and again to ensure that no pilferage of any sensitive information.

No third party vendors, contractors are permitted in restricted zone. Any meeting with this person if required are held at non secured zone office at the front office.