Department		Issue Date	Revision #
SEC	OEC-SEC-UE-P-02	2016-09-21	0.0
	UNATTENDED USER EQUIPMENTS POLICY		Pages 1 of 2

INTRODUCTION

It has been acknowledged by the organization that implementation of discipline is a necessary way to ensuring the User equipments leave unattended and invite Security incidents are dealt with/in a fair and effective way wherever extreme carelessness or apparent irresponsibility is involved.

PURPOSE

The purpose of this policy is to safeguard the information leakage and malpractices resulting due to unattended equipment policy. This policy applies to all the equipments that can cause security concern to any of the information Security Processing Assets.

SCOPE

The procedure applies to all employees regardless of their length of services. This procedure is used to deal with the personnel left user equipments un attended pertaining to Information Security.

REFERENCE

Security Department

HOD-Head of Department

IT-Information Technology

RESPONSIBILITY

Reporting Manager

Head of Department

Security Staffs

ISMS/Concern Manager

Information Technology

Un attended Equipment Policy

User Equipments

- No user equipments like Workstations, requested Medias, laptops, servers should be left unattended or unlocked.
- Workstations / Laptops / Servers desktop screen should comply with the Clear desk and screen policy while unattended.
- Requested media by an employee is sole responsibility of the requester. Employee must follow media handling policy and should not leave the media unattended.
- Media Room should be restricted with stringent Stand alone Bio-metric systems for unauthorized entries.
- To make sure the above Security Personnel must be taken rounds inside the office on a frequent intervals and report to the concerned if any violations noticed.
- While outside the company premises, the devices like Laptops must be protected from physical and information theft.

Other Equipments :

- Devices like Hardware Firewall, Routers, monitoring, access control, Bio-Metric and back up devices should be properly monitored from theft and tampering.

Procedures :

- Workstations / laptops / Servers when not attended should be locked and password protected.
- Auto lock, shutdown of inactive session must be activated.
- Media (Compact Disk, DVD, Floppy, USB Flash drive, External Hard Disk etc.) containing critical information should not be left unattended.
- Any incident of theft or loss must be reported to the management.

Responsibility:

- All the employees are responsible for the equipments allotted to them.
- Management is responsible for security of other devices and equipments.

Effective Date:

This policy will be effective from 21 September 2016.

Violation:

The company expects total compliance of this policy. Violation, if any, will be viewed seriously and may invite appropriate action.

Policy Owner:

Security Department would be responsible for maintaining and carrying out subsequent modifications.

Revision of Policy:

Management reserves the right to revise this policy at any time and in any manner without notice. Any change or revision will be available with the Management and will be communicated appropriately.

ENCLOSURES

NA

FORMATS / EXHIBITS

NA