DEPARTMENT		ISSUE DATE	REVISION #
SEC	**OEC-SEC-AC-P-03**	**2016-09-21**	**0.0**
	ACCESS CONTROL POLICY		PAGES **1 of 4**

INTRODUCTION

It has been acknowledged by the organization that the implementation of the Access Control Policy to make sure to avoid untoward Security incidents are dealt with/in a fair and effective way wherever extreme carelessness or apparent misconduct is involved.

PURPOSE

The purpose of this policy outlines authentication requirements for applications, documents, information, data etc., at working premises. It includes the types of systems that require authentication.

SCOPE

This policy applies to all stakeholders of the organization (staff, contractors, consultants, temporary employee, visitors, etc.) while using organizations computing or networking resources. All users are expected to be familiar with and comply with this policy.

REFERENCE

Security Department
HOD-Head of Department
IT-Information Technology

RESPONSIBILITY

Reporting Manager
Head of Department
Security Staffs
ISMS/Concern Manager
Information Technology

Access Control Policy

Network and System Access – Employees

- The network and system resources that require specific authentication for access are
- File server
- Application server
- Database server
- Firewall (Watch guard X 15)
- Proxy Server
- Email Server
- Backup server
- Access authentication to the above resources will be granted only to the authorized and full time employees of organization.
- The authentication process will permit access to only predefined sections / domains within the listed resources. This access definition is drawn based on the role and function of the employee that determines the level of access required.
- The access ids and passwords are recycled as per Password policy.

All printed copies except the MASTER COPY, *and all electronic copies and versions except* the one accessible on the OEC Intranet Server, *are considered uncontrolled copies used for reference only.*

Network and System Access – Third Party

- Third party access to network and system resources are limited only to those parties explicitly authenticated and configured by the organization. Network administrator. This access configuration is done on a special case basis when demanded by the management as part of the maintenance or service delivery.
- This third party access is open to audit and transaction screening by xxxxx at any time during the engagement.
- An authorized staff member must accompany any third party member accessing the network.

Physical Access – Employees

- Perimeter security mechanism and devices installed at the site provide for the physical access control of the employee movement in and out of the premises.
- Registers / logs of employee movements are maintained and verified on a periodic basis.
- Granting and denying of physical access to employees is under the sole discretion of the management.
- Within the premises the employees' access to zones is determined by their roles and functions.
- Employees are strictly prohibited from entering zones demarcated as "Restricted Access" without prior permission.

Physical Access – Third Party

- Registers of all the third party entering the premises are maintained and verified on a periodic basis.
- For the Visitors and third parties, "Visitor Policy" will be followed.
- Third party visitors to the premises will have to be accompanied by at least one full time member of staff.
- Granting or denying of physical access to third party is under the sole discretion of the management.
- Third party members are strictly prohibited from entering zones demarcated as "Restricted Access" without prior permission.

Operational System Access Control

- Operating systems on the workstations and servers will be password protected and only authorized users will be having an access.
- Every User will create an account with a user name and password following the password policy.
- The user will have to login to their account when the operating system loads.
- Guest account on the operating system will be disabled to avoid any unauthorized access.

All printed copies except the MASTER COPY, *and all electronic copies and versions except* the one accessible on the OEC Intranet Server, *are considered uncontrolled copies used for reference only.*

- The management of the password for the user account will comply with the password policy.
- System utility programs / software's installed on the operating system must comply with the "Acceptable Software Policy".
- Operating systems will be configured to turn off the monitors after 2 minutes of inactivity.
- Connection to the server operating system using VPN will disconnect after 24 hours.
- Remote desktop / desktop sharing utilities will disconnect after 24 hours.

Access authorization to employees will be granted following a formal registration and de-registration procedure.

Internet Access Control Policy

- Usage of Internet will be controlled using Web Blocker functionality within the Hardware Firewall.
- The list of harmful sites will be blocked using the Web blocker service form Watch guard technologies.
- Prevent access to sites that pose network and security risks including spyware, P2P and streaming media sites.
- URL database is updated daily to give you the most current protection available.
- Web access will be configured by users, groups, domains, time of day, and department requirements to meet specific business and user needs.
- List of "allowed" sites will be maintained to keep the mission critical access open
- Acceptable usage policy for internet will be enforced using the web blocker service to protect the business form legal liabilities.
- Graphical reports for web access, usage and time of day will be logged and monitored to take the security decision and Capacity monitoring.

Responsibility:

It will be responsibility of all employees, third party and management staffs to ensure the access control policy is understood and followed.

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 and IT 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