



ACCESS CONTROL POLICY

1.0 **Purpose:**

Access control procedures will cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention shall be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

2.0 **Scope:**

The policy applies to all PCPL employees including, but not limited to full time employees, part-time employees, contractors, temporary workers, trainers, volunteers and anyone else granted access to sensitive information by PCPL. Further, the policy applies to all systems, computer networks and applications as well as facilities which processes, stores or transmits electronic information.

3.0 **Definition:**

PCPL: ProcessLOGIX Consulting Pvt. Ltd.
HOD: Head of Department / Functional Head
ISM: Information Security Manager

4.0 **Responsibility:**

The overall responsibility of implementation of this policy lies with all HODs and ISM.

5.0 **Description:**

The policy consists of the following sections: User/Application Access Management and PC/Laptop Logical Security

- **User/Application Access Management**

- Formal procedures shall be in place to control the allocation of access rights to information systems and Application/services. Users shall be granted access based upon the principle of applying the least privilege required for achieving their desired job function.
- PCPL users shall be granted access to information, data and applications on a "need to know" basis. Access shall be restricted according to the user's requirement to access information, data or application on the basis of least privilege to achieve the desired business function.
- An accurate date and time shall be maintained on all systems
- All access violation attempts (user and resource authentication) shall be logged and reported by Administrator to the next higher authority as deemed appropriate.
- There shall be a one-to-one relationship between user Ids and individuals. Access to computing resources (e.g. files, applications, and databases) via shared User Ids is strictly prohibited unless otherwise authorised in writing by the immediate controlling authority.
- Access is controlled by Active Directory authentication to ensure only properly authenticated users and computers can logon to the network.

- **Password Authentication**
 - Passwords are not shared and treated as confidential information under company policy.
 - Network login automatically becomes locked after three incorrect attempts to input password.
 - Any password used for access must:
 - Use at least 7 characters;
 - Use both upper and lower case characters; and
 - Uses numeral digits.
 - Passwords must be changed periodically and have a maximum use limit of 42 days.
- Users' access rights shall be reviewed at an interval of 6 months. However, authorizations for special privileged access rights shall be reviewed at an interval of 3 months.
- **PC/Laptop logical security**
 - The logical security of PCs/laptops and the security of data residing on these systems shall be ensured.
 - Network router and firewall restricts inbound/outbound access. Network access limited to computers within secure zone and laptop users with VPN access.
 - Administrative access rights disabled on desktops or laptops. Employees are unable to install software or alter user based restrictions.
 - Network access disabled in visitor conference room (Rooms E) and employee cafeteria. Limited internet access using an independent network not connected to the PCPL domain is available.
 - All laptop computers are encrypted.

6.0 References

IM-POL-011 Physical Security Policy

Amendment Control

Amendment Number	Release Date	Section	Page Number	Nature of Change	Authorized by

PREPARED BY: ISM		VERSION NO. : 1.0
APPROVED BY: MD		RELEASE DATE: 01/06/09