**ACCESS CONTROL POLICY**

|  |  |
| --- | --- |
| **Document Name** | **Access Control Policy** |
| **Version** | **0.1** |
| **Last Updated by** | **Anjaly T A** |
| **Approved By** | **Inderjit Singh Bedi** |
| **Released on** | **22-09-2022** |

# Introduction

Information is the critical aspect for any organization’s existence and growth. It is of utmost importance that the policy is defined at organizational level to establish the need to secure information and information processing facilities. Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

# Objective

The purpose of this Policy is to prevent unauthorized access to operating systems. This Policy is designed to protect *information* from unauthorized change, destruction, or disclosure, whether intentional or accidental.

# Scope

The scope of this Policy includes all Xtracap employees. Each employee is responsible for carrying out his or her responsibilities under this Policy.

# Enforcement

Violations of this Policy include but are not limited to: accessing *information and information processing facilities* which the individual has no legitimate access to; enabling unauthorized individuals to access the *information*; disclosing *information* in a way which violates applicable policy, Policy or other relevant regulations or laws; or inappropriately modifying or destroying *information.* Violations may result in access revocation, corrective action up to and including dismissal, and/or civil or criminal prosecution under applicable law.

# Policy for Access Control

It is the responsibility of Staff to protect *information* from unauthorized change, destruction or disclosure.

## Access to information or information processing facilities

* On the first day of joining, System Admin & Human Resource (HR) departments ensure that personnel have computer system ready, inline with Human Resource Security Procedure, User Access Management Procedure and Password Management Policy.
* Access to information and information processing facilities is controlled and restricted as per the role and responsibility of the personnel & the group they’re assigned to:
  + Leadership Group: Access to all the files and groups
  + HR: Mohammed Riaz
  + Marketing: Leadership +Marketing group
  + BA: BA+ QA + Leadership
  + IT Team: All IT Team members + Leadership
  + BDM: All Business development members + leadership

* Access controls are both physical and logical, where physical access control covers controlled physical entry to information & information processing facilities and logical access control covers controlled electronic access to information & information processing facilities:
* These rules are established based on premise “Everything other than rules defined are generally forbidden unless expressly permitted” rather than the weaker rule “Everything is generally permitted unless expressly forbidden”;
* Department-specific rules and rights must be defined, reviewed, and approved by the IT-Infra Head and it is reviewed on a quarterly basis to assess the risks associated with access rights;
* Access control rules and rights for each user and/or group of users are clearly defined and implemented.