|  |  |
| --- | --- |
| **Document Name** | **Access Management Policy** |
| **Version** | **0.3** |
| **Last Updated by** | **Anjaly T A** |
| **Approved by** | **Inderjit Sigh Bedi** |
| **Released on** | **23-08-2022** |

Contents

[1 Introduction 2](#_Toc53496856)

[2 Objective 2](#_Toc53496857)

[3 Scope 2](#_Toc53496858)

[4 Reference 2](#_Toc53496859)

[5 Enforcement 2](#_Toc53496860)

# Introduction

Access management is the process of identifying, tracking, controlling and managing authorized or specified users’ access to a system, application or functionality. In essence, it helps monitor and limit the number of users and their access to different systems and data in the company. There will be a specific hierarchy to the system where a few designations provide the permission to others to view/edit/initiate a process or document.

# **Objective**

The purpose of this Policy is to prevent unauthorized access to different systems and functionalities. It will also delineate a hierarchy through which the users that seek access to a system must go through. The document will also carry the procedure they must follow in order to gain the right to access the system/functionality. The document also lists all the systems/functions/documents that fall under this purview and the ones that can be access by anyone in the company.

# Scope

* The scope of this Policy includes all XTRACAP employees. Each employee is responsible for carrying out his or her responsibilities under this Policy.
* The scope of this policy will also include third parties that will gain access to the app or integrate with any of the services on our system.

# Reference

Procedure / Policy:

The procedure to gain the right to access any of these would be to request access from the approver. The access is defined beforehand and includes - view only, to edit to partially edit. The approver can use his/her discretion to grant the right to access or consult the right authority and then approve/reject/modify the request.

The following list includes (but is not limited to) the roles that are ones that are frequently request for access for folders, systems, functionalities and databases. The roles and the approver mark the relationship between the user that requests access and the one that provides it. Wherever there are two approvers, the former approver will give consent and only then the latter approver will provide the access

|  |  |
| --- | --- |
| Roles | Approver |
| One Drive | IT Infra Head |
| Developers | IT Lead and IT Infra Head |
| Quality Analysts | IT Lead and IT Infra Head |
| Business Analysts | IT Lead and IT Infra Head |
| Marketing | IT Infra Head |
| Risk Management | Senior Management |
| Strategic and Partnership | Senior Management |
| Executives | IT Infra Head and Risk Manager |
| Third Parties | IT Lead and IT Infra Head |

# Enforcement

Violations of this Policy include but are not limited to: accessing information and information processing facilities to which the individual has no legitimate access; 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.