INSERT LOGO

ACCESS CONTROL POLICY

Classification: **Internal**

Without the owner's written approval, this document may not be shared with anyone outside of [Company Name].

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

CONTENTS

Contents....1
Purpose of Document....1
Scope....2
Responsibilities....2
Managers:....2
Access control....2
User Access Account Management....2
Change of status or termination of contract....2
Privileged Account Management....3
Separation of Permissions....3
Principle of Least Privilege....3
Regular review of access rights....3
User password management....3

PURPOSE OF DOCUMENT

This document outlines the policy for controlling system access balancing business and security needs.

SCOPE

This policy covers all on-site and cloud-based systems. It targets managers, system owners, the IT department, and administrators overseeing [Company Name] data.

RESPONSIBILITIES

MANAGERS:

- Ensure staff have essential system access for their roles.
- Authorise individual access to apps and data.
- Immediately communicate and adjust access rights for role changes or departures.
- Regularly (quarterly) review staff access levels

System Owners & Privileged Users:

- The system owner manages and upholds the policy if access rights fall outside IT.

IT Help Desk:

- Grant system access and review access anomalies.

ACCESS CONTROL

USER ACCESS ACCOUNT MANAGEMENT

- Each user has a single non-admin account per system; exceptions need approval.
- User IDs are personal and unique.
- Avoid generic accounts, especially for sensitive data, as they hinder auditability.
- Under no circumstances should generic accounts be created for any administrative accounts or accounts that access privileged and sensitive material, including information relating to people, as it inhibits the ability to audit who made what changes and when.
- Procedures for user registration, modification, and de-registration are essential.
- Manager or system owner authorisation is needed for system access.
- Access rights must adapt to business changes, role shifts, or user departures.
- Document all changes to access in a log.
- Only trained employees should implement user management.
- Establish access standards for each system without hindering work.
- Use Multi-Factor or 2 Factor Authentication for enhanced security.
- Implement Single Sign-On (SSO) for centralised access rights.

CHANGE OF STATUS OR TERMINATION OF CONTRACT

- Inform HR, IT, and other departments about role changes or departures.

- Contract alterations with external parties should be communicated to system privilege managers.

PRIVILEGED ACCOUNT MANAGEMENT

- Log all privileged account changes.
- Avoid generic admin accounts to maintain auditability.
- Base all admin and privileged user accounts on job roles.

SEPARATION OF PERMISSIONS

- Admins should maintain separate general and privileged accounts.

PRINCIPLE OF LEAST PRIVILEGE

- Grant users only essential access rights for their roles.

REGULAR REVIEW OF ACCESS RIGHTS

- Audit accounts quarterly to deactivate used ones.

USER PASSWORD MANAGEMENT

- Ensure all [Company Name] systems have a user ID and password in line with [Company Name] 's password policy.