[Company Logo]

Privileged User Management Policy

To ensure the security of company data by establishing requirements for the proper maintenance and oversight of privileged user accounts and access within the organization's IT environment.

Document Owner
Head of IT/Security

[Company Logo]	**CONTROLLED DOCUMENT** **Privileged User Management Policy**	Document: Privileged User Management Policy Developed by: Reviewed by: Approved by:

Privileged User Management Policy
For

[Company Name].

Version: 1.0
Date: 01/01/0000
Next Review Date :

Note: Verify with the Policy Owner if this is the correct and latest version before use.

Revision History

Rev. #	Date	Modification Details	Page#	Suggested By	Reviewed By	Approved By
1.0		First Draft	NA			

[Company Logo]	**CONTROLLED DOCUMENT** **Privileged User Management Policy**	Document: Privileged User Management Policy Developed by: Reviewed by: Approved by:

Table of Contents

[Company Logo]	**CONTROLLED DOCUMENT** **Privileged User Management Policy**	Document: Privileged User Management Policy Developed by: Reviewed by: Approved by:

Purpose

Privileged access management (PAM) policy is a cybersecurity strategy and technology for exerting control over the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment. By dialing in the appropriate level of privileged access controls, PAM helps organizations condense their organization's attack surface and prevent, or at least mitigate, the damage arising from external attacks as well as from insider malfeasance or negligence.

Scope

This Privileged Access Management Policy applies to all individuals, systems, and processes within [Company Name] that involve elevated or administrative access rights. It encompasses:

- Users: Employees, contractors, vendors, and third parties with privileged access to systems, applications, databases, or network infrastructure.
- Accounts: All privileged accounts, including administrative, root, service, and emergency access accounts.
- Systems: On-premises infrastructure, cloud environments, endpoints, and any IT resources requiring privileged access.
- Processes: Creation, approval, monitoring, rotation, and revocation of privileged access.

The policy ensures strict controls over privileged access to mitigate risks of misuse, data breaches, and insider threats

Objective

This policy defines the requirements surrounding the creation, use, monitoring, and decommissioning of privileged user accounts within the company data network.

Responsibility & Accountability

1. Privileged Users
    - Must adhere to the principle of least privilege and use elevated access only for authorized tasks.
    - Are responsible for securing credentials, reporting suspicious activities, and never sharing privileged accounts.
2. IT Security Team
    - Implements and maintains PAM controls (e.g., MFA, session monitoring, password vaulting).
    - Conducts regular audits of privileged access and reviews compliance with this policy.
3. Data/System Owners
    - Approve or revoke privileged access requests based on business justification.
    - Ensure access aligns with job responsibilities and is time-bound.
4. CISO/IT Leadership
    - Oversees PAM program effectiveness and policy enforcement.
    - Reports policy violations to executive management and HR for disciplinary action.
5. HR & Third-Party Managers
    - Ensure timely revocation of access for employees/contractors upon role changes or offboarding.

Non-Compliance

Any Non-Compliance with this Privileged access management policy will be dealt with Disciplinary Action as decided by the organization and respective authorities.

Exceptions

Not Applicable.

Policy Statement

1. These accounts should be created with a standard naming convention that will serve to distinguish them from a normal user account. At the same time, identify the individual to whom the account has been assigned.

2. Authorization for the creation of a privileged account must be submitted in writing by the appropriate Data Owner and approved by the Chief Information Officer.

3. Each request for privileged access must include an appropriate justification for the request as well as an expiration date.

4. Enforce password security best practices:
   - Change the password on each device so you are not using the default password.
   - Require privileged account passwords to be changed regularly to reduce the risk of departing employees compromising your systems.
   - Eliminate password sharing; each account should have a unique login to ensure clear oversight and a clean audit trail.
   - Ensure robust passwords that can resist common attack types (e.g., Brute force) by enforcing strong password creation parameters, such as password complexity, uniqueness, etc

5. Multifactor Authentication Requirements:
   A password alone is not enough. Options include hard tokens, soft tokens, NFC, Bluetooth beacons, GPS, and fingerprints.

6. Many privileged accounts have no limits, they have full access to everything:
   - Separation of duties- No employee can perform all privileged actions for a given system or application
   - Least privilege- Employees are granted only the bare minimum privileges needed to perform their jobs.

7. Ideally, each admin should have only one privileged account for all systems.

8. With more workflows shifting to the cloud each year, the same privileged access management best practices need to be used for accounts that give privileged access to cloud-based on-premises systems and services and services, such as Azure Active Directory accounts.

9. Educate users: Give your staff the information they need to succeed, and be sure to update them about policies and procedures whenever there is a change to their daily routine.

Conclusion

This document provides an overview of the privileged user management policy & its deliverables, the project team participants, and their roles and responsibilities. It is intended to assist Application Managers and developers of [Company Name] applications and to ensure a consistent approach to privileged user account management.

<<< End of Document >>>