Privileged Account Management Document

Document Version: 1.0
Date: [Date]
Prepared by: [Name/Team]
Organization: [Company Name]

1. Purpose

This document provides an overview of privileged account management (PAM) practices and standards for enterprise environments to mitigate risks associated with the misuse of powerful accounts.

2. Scope

This policy applies to all privileged accounts within the organization’s IT environment, including but not limited to domain administrators, server administrators, database administrators, network device administrators, and application super users.

3. Definitions

- **Privileged Account:** Any account with elevated permissions that enable the holder to make significant changes to IT systems, applications, or network devices.
- **PAM:** Privileged Account Management, the processes and technologies used to manage and monitor privileged accounts.

4. Roles and Responsibilities

Role	Responsibilities
Account Owner	Ensures all privileged accounts in their domain are used appropriately and complies with policy.
IT Security	Monitors, audits, and reports privileged account usage. Reviews PAM controls regularly.
System Administrators	Implements PAM solutions and ensures adherence to management process.

5. PAM Controls and Processes

1. **Account Inventory:** Maintain an up-to-date inventory of all privileged accounts.
2. **Least Privilege Principle:** Assign the minimum necessary privileges required for each role.
3. **Approval Workflow:** Require documented approval for creating, modifying, or deleting privileged accounts.
4. **Password Management:** Enforce strong password policies and regular password changes.
5. **Multi-Factor Authentication (MFA):** Require MFA wherever possible for privileged access.
6. **Session Monitoring:** Monitor and, where feasible, record sessions of privileged activities.
7. **Regular Review:** Conduct periodic reviews and recertification of privileged accounts and their permissions.
8. **Audit Logs:** Enable and retain audit logs of all privileged activities for compliance and investigation.
9. **Emergency Access:** Define and document procedures for emergency privileged access ("break glass" procedures).

6. Incident Management

All suspected misuse or compromise of privileged accounts must be reported immediately to IT Security. Incidents will be investigated in accordance with the organization’s incident response plan.

7. Compliance & Review

This document and related controls will be reviewed annually or as required due to significant environmental or regulatory changes.

8. References

- [Reference 1 - e.g., NIST Guidelines]
- [Reference 2 - e.g., Internal Security Standards]
- [Reference 3 - e.g., ISO/IEC 27001]

9. Document History

Version	Date	Changes	Author
1.0	[Date]	Initial draft	[Name/Team]