🛡️ Sampurna Vault – Security Policies & Guidelines

Strict Usage Rules & Compliance Standards

1. General Security Rules (For All Users)

These rules apply to every employee, regardless of their role.

A. Password & Authentication Policy

1. **Strict Confidentiality:** Never share your Vault password or OTP with anyone, including IT staff or managers.
2. **Password Strength:** When prompted to change your password, ensure it is at least **8 characters long** and includes a mix of letters, numbers, and symbols.
3. **2FA Mandate:** Two-Factor Authentication (OTP via Authenticator App) is mandatory. Disabling 2FA is a violation of security policy.
4. **Lock Your Screen:** Never leave your computer unlocked while logged into the Vault.

B. Device & Network Security

1. **Official Devices Only:** Do not access the Vault from personal devices (café computers, personal tablets, unmanaged phones).
2. **Phishing Awareness:** The Vault URL is https://4.187.152.147:8200. Verify this URL every time before entering credentials.

2. Guidelines for Normal Users

Role: Standard Employees managing personal secrets.

A. Allowed Data

1. **Work-Related Only:** The mysecret folder is for storing **work-related** credentials only (e.g., Jira passwords, internal portal logins).
2. **No Personal Data:** Do not store personal banking passwords, social media logins, or private photos in the company Vault.

B. Data Hygiene

1. **No Excel Sheets:** You are strictly prohibited from saving passwords in Excel files, Sticky Notes, or Notepad on your desktop. Move them all to Vault.
2. **Copy-Paste Security:** When copying a password from Vault, clear your clipboard immediately after usage.

C. Incident Reporting

1. **Lost Device:** If you lose the phone containing your Authenticator App, report it to IT **immediately** so your OTP access can be revoked.
2. **Suspicious Activity:** If you see a "Last Login" time that you do not recognize, notify IT immediately.

3. Guidelines for Super Users

Role: Senior staff managing shared company secrets (scripts engine).

A. Secret Management & Hierarchy

1. **Naming Convention:** You must strictly follow the folder hierarchy.
    a. ☑ Correct: scripts/prod/aws/billing-key
    b. ❌ Incorrect: scripts/my-stuff/key1
2. **Least Privilege:** Do not give a secret path to a junior developer unless they specifically need it for a task.
3. **No Hardcoding:** Do not copy credentials from Vault and hardcode them into application source code. Applications should be configured to fetch secrets dynamically or via environment variables.

B. Operational Integrity

1. **Version Control:** If you update a password (e.g., Database Rotation), verify the application is working before closing the session. Vault keeps versions—use the **Rollback** feature if the new password fails.
2. **Rotation Policy:** Critical production secrets (e.g., AWS Root Keys, Database Master Passwords) should be rotated every 90 days.

4. Guidelines for Administrators (IT Admin)

Role: System Owners managing the VM, Keycloak, and Vault Server.

A. Root Token Security

1. **Absolute Secrecy:** The **Vault Root Token** allows full access to everything. It must **never** be shared via chat or email.
2. **Storage:** Store the Root Token in a secure, offline location (e.g., a physical safe or an encrypted offline drive).
3. **Script Hygiene:** When running Python bulk scripts (delete_vault_folders.py), **never commit the script to Git** with the Root Token inside. Delete the token from the script immediately after running it.

B. Server Maintenance

1. **Unseal Keys:** The 3 Unseal Keys must be distributed among different senior admins. No single person should hold all keys if possible (Split Knowledge Principle).
2. **Backups:** Perform daily snapshots of the VM or specific backups of the Vault data directory.
3. **Audit Logs:** Review Keycloak and Vault audit logs weekly to detect failed login attempts or unauthorized access patterns.

C. Onboarding & Offboarding

1. **SLA for Removal:** When an employee leaves, their access must be revoked (User deleted in Keycloak) within **1 hour** of their exit.
2. **Clean Up:** Run the Vault cleanup script (delete_vault_folders.py) promptly to ensure no stale data remains for terminated employees.

5. Violation & Enforcement

Failure to adhere to these guidelines poses a risk to Sampurna's data security.

1. **First Violation:** Formal warning and mandatory security retraining.

2. **Second Violation:** Temporary suspension of Vault access.
3. **Severe Violation:** (e.g., sharing the Root Token or exporting secrets to public networks) will result in immediate disciplinary action, up to and including termination of employment.

6. Summary