User Access Guidelines for Compliance Auditing

Version: 1.0
Last Updated: [Insert Date]
Document Owner: [Insert Owner Name]
Reviewed By: [Insert Reviewer Name]

---

1. General Access Rules

- **All users** must follow **Role-Based Access Control (RBAC)**.
- Users should **only** have access to **data and systems relevant to their job**.
- Any **access modification requests** must be **approved by a supervisor**.

---

2. Terminated Employees

- **Action Required:** Accounts of terminated employees **must be deactivated within 24 hours**.
- **Violation:** If a terminated employee retains access after 24 hours, it must be escalated to security.
- **Policy:** No terminated employee should have **access to internal systems or company data**.

---

3. Contractors & Temporary Workers

- **Contractor Access:** Contractors should have **limited access to only project-related data**.
- **Access Expiry:** Contractor accounts must be **time-restricted and revoked automatically upon project completion**.
- **Security Measure:** Contractors must use **separate guest accounts** (not employee credentials).

---

4. Admin & Privileged Access

- **Data Restriction:** Admins should **only access systems for administration tasks**.

- **HR & Finance Data:** Admins **must not access personal employee records**.
- **Privilege Escalation:** Any **admin access change requests** must be **logged and approved**.
- **Security Measure:** Admin accounts must require **Multi-Factor Authentication (MFA)**.

---

5. Remote Access & VPN Policies

- **VPN Usage:** Remote employees must use a **company-approved VPN**.
- **Monitoring:** All **VPN sessions must be logged and reviewed**.
- **Unauthorized Access:** If an employee logs in from **an unapproved location**, access should be revoked.

---

6. High-Security Data & Protection Policies

- **Data Storage: Confidential data should only be accessed from company-secured devices**.
- **Training Requirement: HR, Finance, and Legal employees must undergo annual security training**.
- **Data Transfer Restriction:** Employees cannot **download sensitive data to personal devices**.

---

7. Multi-Factor Authentication (MFA) Policies

- **Mandatory: All employees must enable MFA** for account security.
- **Violation Handling:** Any account without MFA must be **flagged for review**.
- **Security Alert:** If an employee fails **MFA authentication more than 3 times**, security must be notified.

---

8. Inactive Accounts

- **Auto Deactivation:** User accounts inactive for **90+ days must be automatically disabled**.
- **Supervisor Approval:** Any account **re-activation must be approved** by a supervisor.

🛠 Compliance Monitoring & Auditing

Auditing Process:

- **Access logs** should be reviewed **weekly** for any violations.
- **Automated alerts** should notify security for any unauthorized access attempts.
- **Audit Reports** must be generated every **month** for compliance tracking.

📝 Notes:

- This document is **subject to periodic review**.
- Any **policy updates** must be communicated to **all employees and contractors**.
- **Violations of these guidelines may result in access revocation or disciplinary action**.