# Umay Solutions – User Access Management (UAM) Policy & Procedures

**Document ID:** UAM-PL-001  
**Version:** 3.0 (Detailed)  
**Status:** Draft  
**Owner:** Chief Risk & Compliance Officer (CRCO)  
**Approved By:** Board Risk & Compliance Committee  
**Effective Date:** TBD  
**Review Cycle:** Annual (or sooner upon significant change)

## 1 Purpose

This document establishes Umay Solutions’ minimum requirements for creating, modifying, reviewing, and removing user access to all corporate information systems and data. Its objectives are to:  
\* Protect the confidentiality, integrity, and availability of information assets.  
\* Ensure access privileges are consistent with job responsibilities (least‑privilege).  
\* Provide accountability through auditable, well‑defined processes.  
\* Comply with applicable regulatory and contractual obligations (e.g., ISO 27001, PCI DSS, SOC 2).

## 2 Scope

**Applies To**  
\* All permanent and temporary employees, interns, contractors, consultants, and third‑party service providers who require logical or physical access to Umay Solutions’ facilities, systems, applications, or data.  
\* All computing environments (production, test, development), endpoints, SaaS services, and on‑premises infrastructure.  
\* All data classifications, with heightened control requirements for *Restricted* and *Highly Restricted* data.

## 3 Key Principles

1. **Unique Identity** – every person or service has a unique identifier; shared accounts are prohibited unless explicitly approved and documented.
2. **Least Privilege** – users receive only the permissions required to perform their duties, for the minimum necessary duration.
3. **Segregation of Duties (SoD)** – duties that, when combined, may allow a single individual to subvert controls must be separated.
4. **Timely Revocation** – access is revoked immediately when no longer required.
5. **Accountability & Auditability** – every access event and change is fully documented, approved, and retained for audit.

## 4 Roles & Responsibilities

| Role | Responsibilities |
| --- | --- |
| **Board Risk & Compliance Committee** | Approves this policy and reviews quarterly status reports. |
| **Chief Risk & Compliance Officer (CRCO)** | Owns policy; approves privileged and SoD‑sensitive access; reviews exceptions. |
| **Chief Technology Officer (CTO)** | Ensures technical feasibility; allocates resources for implementation. |
| **Chief Data & AI Officer (CDAO)** | Oversees data governance, analytics, and AI model operations. |
| **VP FP&A** | Oversees financial planning and analysis, including department-level access approvals. |
| **Information Security (GRC Team)** | Maintains SoD matrix; oversees quarterly reviews; monitors KPIs; performs spot checks. |
| **IT Operations – Access Administration Team** | Executes provisioning and de‑provisioning; maintains the *Access Register* and *Privileged Access Log*; verifies documentation. |
| **Line Managers (Requestors / Approvers)** | Request, justify, and approve access for direct reports; re‑certify access quarterly; validate removals. Must not be the same as the provisioner. |
| **Human Resources (HR)** | Provides authoritative joiner, mover, and leaver notifications. |
| **Third‑Party Sponsors** | Ensure vendor users are requested, monitored, and promptly removed. Contract extension or scope changes must be reflected in updated requests. |
| **Internal Audit** | Independently assesses compliance with this policy. |
| **All Users** | Safeguard credentials; use only assigned accounts; report suspicious activity. |

**Expanded Reporting Structure (Key Roles Below Management Level):**

[… existing role structure retained …]

## 5 Access Lifecycle Management

### 5.1 Joiners (New Users)

* All new users must be requested using the **New User Access Request Form (NUARF)** submitted by the hiring or sponsoring manager.
* All new users must be requested by the hiring or sponsoring manager.
* The UARF must clearly list the user’s department, job title, and specific role-based access being requested.
* Approvers must be from the approved list defined in the UAM Approver Matrix. This includes Line Managers, Department Managers, and any personnel holding a Manager, Head, VP, or C-Level title within the relevant functional area.
* For non-employees (e.g., vendors/contractors), start and end dates must be defined. Standard access duration for contractors is 12 months unless otherwise justified.
* Emergency access requests must include the exact permissions requested and be pre-approved by CRCO or delegate. No access may be created without explicit approval.
* All new user requests are logged in the *Access Register*, including approver details and timestamps.
* Provisioning is performed by the Access Administration Team. Final verification is conducted to ensure access matches the approved request.
* All provisioners are logged. The system captures the user ID, provisioned roles, and the provisioner’s name and timestamp.

### 5.2 Movers (Access Changes)

* Any change to user access must be initiated using the **User Access Change Request Form (UACRF)** submitted by the user’s Line Manager.
* Any change to access is initiated using a Change Access Request Form (CARF).
* CARF must specify all permissions to be added, removed, or changed.
* Approval must come from a designated manager who is not the modifier.
* Approvals and changes are logged in the *Access Register*.
* Emergency access modifications follow the same emergency protocol as new access and must be approved before action.
* Provisioning team performs changes and records who made the modification.
* System logs all changes for audit trail. Final check is conducted to confirm changes match approved modifications.
* Access granted must align with the user’s new responsibilities and avoid SoD conflicts, validated through the SoD matrix.

### 5.3 Leavers (Terminations)

* Access removal must be triggered by a leaver notification from HR.
* Standard SLA for removal is within 1 business day of effective date.
* Termination access logs are retained for audit.

### 5.4 Temporary & Emergency Access

* Emergency access must be pre-approved by the CRCO or a delegated authority.
* The request must include specific roles and privileges being granted.
* Emergency access may never be provisioned without an approval.
* Access is always time-bound and logged in the *Emergency Access Register*.
* A post-review is conducted by GRC to validate access alignment with justification.

## 6 Privileged Access & SoD Conflicts

* Any account with elevated privileges (e.g., admin, deployment, security) must be individually approved by the CRCO.
* Privileged access assignments are reviewed quarterly.
* Segregation of Duties (SoD) Matrix maintained by the GRC Team is used to identify and prevent conflicts.
* No individual may approve and provision the same access.
* Users may not grant access to themselves under any circumstance.
* Final validations confirm all access granted or modified aligns with the user’s responsibilities and matches the approval forms.

## 7 Access Reviews and Audit

* Access recertification is conducted every 3 months by Line Managers.
* Privileged access is reviewed monthly.
* Internal Audit may conduct unannounced spot checks on high-risk systems.
* All approvals and access logs must be retained for 12 months (minimum).
* The Access Administration Team is responsible for reconciling system logs against approved access forms.

## 8 Policy Exceptions

* Exceptions to this policy must be documented, reviewed by Information Security, and approved by the CRCO.
* All exceptions are logged and reviewed periodically to ensure risk remains within acceptable levels.

## 9 Policy Maintenance

* This policy is reviewed annually by the CRCO in consultation with Information Security, Legal, and key department heads.
* Any amendments are submitted to the Board Risk & Compliance Committee for review and approval.
* All changes to this document are version controlled. Historical versions are retained for a minimum of three years.

## 10 Non-Compliance

* Violations of this policy may result in disciplinary action, up to and including termination.
* Where applicable, breaches may be escalated to regulators, clients, or legal authorities, particularly in the case of data compromise or unauthorized access to sensitive systems.
* Exception requests must be submitted in writing to the CRCO and will only be granted based on a documented risk acceptance or compensating control.

## 11 References

* ISO/IEC 27001:2022 – Information Security Management
* NIST SP 800-53 Rev. 5 – Access Control (AC) Family
* SOC 2 Trust Services Criteria
* Umay Solutions: Data Classification Policy, Information Security Policy, HR Onboarding Policy

## 12 Document History

| Version | Date | Description | Approved By |
| --- | --- | --- | --- |
| 1.0 | 2024-01-15 | Initial draft | CRCO |
| 2.0 | 2024-07-01 | Included access lifecycle and SoD updates | CRCO |
| 3.0 | TBD | Full compliance update based on audit/control questions and org changes | Board Risk & Compliance Committee |

This policy ensures that all new, modified, emergency, and terminated access is handled according to documented processes, segregation of duties is maintained, and access granted is commensurate with job role. All steps are logged and reviewed periodically to meet regulatory, security, and operational requirements.