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.
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.
Human Resources (HR)	Provides authoritative joiner, mover, and leaver notifications.
Third-Party Sponsors	Ensure vendor users are requested, monitored, and promptly removed.
Internal Audit	Independently assesses compliance with this policy.
All Users	Safeguard credentials; use only assigned accounts; report suspicious activity.

5 Access Lifecycle

5.1 Provisioning (Joiner & Access Changes)

Step	Description
1. Request	The Line Manager completes an **Access Request Form (ARF)** which captures: employee ID, job title, start date, requested systems, specific roles/permissions, business justification, and whether privileged access is required.
2. Approval Workflow	1) Line Manager → 2) Role/Data Owner (if applicable) → 3) CRCO (only for privileged or SoD-sensitive requests) → 4) IT Operations validation. All approvals are dated and signed (wet or digital).
3. SoD Check	IT Operations reviews request against the *SoD Conflict Matrix*. Conflicts must be remediated (split duties) or risk-accepted by CRCO with compensating controls.

Step	Description
4. Provisioning	Access Administration Team creates accounts, assigns groups/roles, sets initial strong password (one-time), and records details in the *Access Register* (controlled spreadsheet).
5. Notification	Credentials are delivered securely to the Line Manager and user (face-to-face, encrypted email, or sealed envelope); user must change password at first log-in.
6. Verification	Line Manager validates correct access within 48 hours; discrepancies reported to IT Operations immediately.
7. Documentation	ARF and provisioning evidence are filed in the *Access Records* repository; retention: 7 years.

5.1.1 Non-Employee Provisioning (Vendors / Contractors)

- Follows the same ARF workflow.
- Requires explicit *Contract End Date* (maximum 12 months).
- Sponsor is responsible for quarterly re-validation of access.
- Accounts automatically expire on contract end date and are disabled within 1 hour.

5.2 De-Provisioning (Leaver & Role Changes)

Step	Description
1. Notification	HR emails the daily **Leaver Report** to IT Operations; urgent terminations are phoned through immediately.
2. Immediate Disable (≤ 1 hour)	Access Administration disables network, email, VPN, and building badge.
3. Full Removal (≤ 24 hours)	All application accounts and group memberships removed; tokens and certificates revoked; privileged credentials rotated.
4. Validation	Line Manager confirms no residual access and that data hand-over is complete.
5. Record Update	*Access Register* updated; removal evidence archived for 7 years.

5.3 Segregation of Duties (SoD)

Conflict Example	Enforced Separation
Payment Creator vs Payment Approver	Two distinct user IDs; cross-approval in payment system.
Developer vs Production Deployment	Developers cannot deploy code; separate Release Engineer role required.

Conflict Example	Enforced Separation
Security Administrator vs System Auditor	Security Admin cannot disable logs; audit role read-only.
User Admin vs Payroll Processing	Payroll Manager cannot assign their own access.

- SoD matrix reviewed at least annually or upon major process change.
- Violations detected during provisioning or quarterly recertification must be resolved within 10 business days.

5.4 Privileged-Level Access

Topic	Requirement
Profiles	Domain/Admin, Database SysAdmin, Network Infra Admin, Security Admin, Application Superuser, Emergency Break-Glass.
Eligibility	Staff must: (a) have a business need; (b) complete Privileged Access Training; (c) sign the **Privileged Access Agreement**.
Approval	Written approval from Line Manager and CRCO; valid for up to 12 months (renewable).
Account Setup	Separate named admin account; password length $\geq$ 15 chars, complexity enabled; MFA mandatory.
Use & Monitoring	Admins log in only for privileged tasks; every session start/end recorded in the *Privileged Access Log*; logs reviewed weekly by Information Security.
Password Management	Changed after first use, every 30 days, or immediately after suspected compromise.
External Vendors	Temporary named admin account; expiry date $\leq$ 30 days; sponsor monitors work; activity logged.
Emergency Access	Break-Glass account held in sealed envelope / digital vault; dual-custody checkout; CRCO review within 24 hours of use.

5.5 Periodic Recertification

Activity	Frequency	Responsible
Standard User Access Review	Quarterly	Line Managers & Information Security
Privileged Access Review	Quarterly	CRCO & Information Security
SoD Conflict Review	Quarterly	Information Security
Third-Party Account Review	Quarterly	Third-Party Sponsors

Results, remediation actions, and approvals are documented and stored in the *Access Review Archive* for 7 years.

---

6 Metrics & KPIs

KPI	Target	Escalation Threshold
Access requests completed ≤ 2 business days	≥ 95 %	< 90 % monthly
Critical de-provisioning within 1 hour	100 %	Any miss escalated same day
Privileged access recertified on schedule	100 %	< 98 %
SoD conflicts unresolved > 10 days	0	≥ 1 escalated to CRCO
Dormant privileged accounts (> 30 days)	0	≥ 1 escalated to CTO

---

7 Enforcement & Exceptions

Non-compliance with this policy may result in disciplinary action up to and including termination, civil liability, and/or criminal prosecution.
Any exception must be:
1. Documented in an **Exception Request Form**.
2. Approved by CRCO.
3. Time-bound with expiry date.
4. Subject to compensating controls.

---

8 Document Maintenance

- **Owner:** CRCO – responsible for keeping this document current.
- **Change Log:** Maintained in the document header.
- **Storage:** Secure share `\Policies\InfoSec\UAM`.
- **Retention:** Superseded versions kept for 7 years.

Appendix A – Access Request Form (ARF)

Required fields: User Name, Employee ID, Job Title, Manager, Start Date, System, Role/Group, Privileged (Y/N), Business Justification, Approvals, Date Provisioned, Ticket Ref.

Appendix B – Privileged Access Agreement (Excerpt)

- I acknowledge responsibility for actions taken using my privileged account.
- I will use the account only for authorised tasks and log out immediately after.

• I will not share credentials.
• I consent to continuous monitoring and recording of privileged sessions.

Appendix C – Access Register (Minimum Fields)

User ID | Name | Department | Role | System | Access Level | Date Granted | Approver | Date Removed | Notes

Appendix D – SoD Conflict Matrix (Sample)

Conflict ID	Role A	Role B	Control Required
SOD-01	Payment Creator	Payment Approver	Two-person approval in system
SOD-02	Developer	Production Deployer	Release Engineer deploys
SOD-03	Security Admin	Log Auditor	Logs read-only for Admin

End of Document