Joiner, Mover, Leaver (JML) Process- WiboCore Bank

1. Purpose

This document defines the Joiner, Mover, Leaver (JML) process for managing user identities and access at WiboCore Bank.

The objective is to ensure:

- Timely and accurate access provisioning
- Enforcement of least privilege and separation of duties
- Immediate revocation of access upon termination
- Full auditability of identity lifecycle events

2. Scope

This process applies to:

- All employees (full-time, contractors, interns)
- All systems within scope:
    - Email (Microsoft 365)
    - CRM (Salesforce)
    - HR System
    - Finance System
    - GitHub
    - VPN
- All identity types:
    - Human users
    - Service accounts (where applicable)

3. Source of Truth

The **HR System** is the authoritative source for identity data.

All lifecycle events originate from HR:

- New hire creation
- Role/department changes
- Termination

No access provisioning or deprovisioning occurs outside this system.

4. Roles and Responsibilities

Role	**Responsibility**
HR Team	Creates and updates employee records
Hiring Manager	Approves access for new hires
Line Manager	Approves access changes (Movers)
Security Team	Reviews privileged access and enforces policies
IT/System Admin	Executes provisioning and deprovisioning
Auditor	Reviews logs and compliance

5. Joiner Process (Onboarding)

Trigger

A new employee record is created in the HR system.

Workflow

1. HR creates employee profile
2. System assigns:
    - Role
    - Department
    - Manager
3. IAM process is triggered:
    - User account created

    - Role-based access assigned (from Access Matrix)
    - Attribute-based policies applied
4. Manager approval required for:
    - Any elevated or non-standard access
5. Security approval required for:
    - Privileged roles (e.g., DevOps, System Admin)
6. MFA enforced at first login
7. User receives onboarding credentials and instructions

Example

Junior Developer

- Email → W
- GitHub → W
- VPN → W
- Finance System → NA

SLA

- Account provisioning completed within **24 hours before start date**

6. Mover Process (Role Change)

Trigger

Change in role, department, or manager in HR system.

Workflow

1. HR updates employee record
2. IAM system detects change
3. Access recalculated:
    - Remove old role permissions
    - Assign new role-based access

4. Manager approval required
5. Security approval required for privileged access
6. All changes logged

Key Control

No Access Accumulation Policy

Users must not retain access from previous roles unless explicitly approved.

Example

Accounts Payable → Finance Manager

- Remove: Write-only finance permissions
- Add: Admin-level finance access

SLA

- Access changes completed within **4–8 hours**

7. Leaver Process (Offboarding)

Trigger

Employee status updated to “Terminated” in HR system.

Workflow

1. Account immediately disabled
2. Active sessions terminated
3. VPN access revoked
4. Tokens/API keys invalidated
5. User removed from all access groups
6. Manager confirms:
    - Ownership transfer of files
    - Handover completion
7. Security logs event for audit

SLA

- Account deactivation: **Immediate (≤5 minutes)**

Risk Mitigation

Prevents:

- Unauthorized access after termination
- Data exfiltration
- Insider threats

8. Special Cases

Contractors

- Must have defined **end date** at onboarding
- Access automatically revoked upon expiry

Privileged Access (JIT Model)

- Admin access granted temporarily
- Requires:
    - Manager approval
    - Security approval
- Automatically revoked after session

Service Accounts

- No interactive login allowed
- Credentials rotated every 30 days
- Access limited to required systems only

Emergency Access (Break-Glass)

- Used only during critical incidents
- Requires post-use audit review

9. Approval Workflow Model

Access Type	Approval Required
Standard Role Access	Line Manager
Cross-Department Access	Line Manager + System Owner
Privileged Access	Line Manager + Security
Finance Admin Access	Finance Manager + Security

10. Audit and Monitoring

All JML activities are logged, including:

- Account creation
- Role changes
- Access removals
- Failed provisioning events

Review Process

- Quarterly access reviews
- Monthly privileged access reviews
- Audit logs retained per compliance requirements

11. Key Metrics (KPIs)

- 100% of users provisioned via HR-triggered workflows
- 0 orphaned accounts
- Deprovisioning within SLA (≤5 minutes)
- No unauthorized privilege escalation

12. Conclusion

The JML process at wiboCore Bank ensures that user access is provisioned, modified, and revoked in a controlled, auditable, and secure manner.

By integrating HR as the source of truth, enforcing role-based access control, and implementing strong approval workflows, the organization minimizes risk while maintaining operational efficiency.

This model reflects real-world IAM practices used in regulated fintech environments.