WiboCore Bank Access Control Matrix

Purpose

This document defines the access control matrix for WiboCore Bank. It specifies which roles have access to systems, applications, and data resources, ensuring secure and appropriate access across the organization.

This document supports:

- Security audits
- Compliance requirements (PCI-DSS, SOC 2, GDPR)
- Internal IAM governance

Document Information

- **Document Owner:** IAM Team (Security Department)
- **Version:** 1.0
- **Last Updated:** April 2026

Overview

The access control matrix below defines access permissions assigned to roles within WiboCore Bank based on the principle of least privilege and separation of duties (SoD).

Legend

- **R:** Read
- **W:** Write
- **A:** Admin (Full Control)
- **L:** Limited
- **NA:** No Access

Access Control Table

Role	Email	CRM	HR System	Finance System	GitHub	VPN	Justification
CEO	W	R	R	R	NA	W	Executive oversight without admin risk
HR Manager	W	NA	A	NA	NA	W	Full HR lifecycle management
HR Specialist	W	NA	W	NA	NA	W	Employee record maintenance

Developer	W	NA	NA	NA	W	W	Code contribution and collaboration
Senior Dev	W	NA	NA	NA	W	W	Advanced development work
DevOps Eng	W	NA	NA	NA	A	W	CI/CD and infrastructure deployment
Finance Manager	W	NA	R	A	NA	W	Financial control and oversight
Accounts Payable	W	NA	NA	W	NA	W	Payment processing only (No approvals)
Accountant	W	NA	NA	W	NA	W	Financial transaction handling
Security Analyst	R	R	R	R	NA	W	Monitoring and incident detection
Auditor	R	R	R	R	NA	NA	Independent audit (no operational access)
IT Support	W	NA	R	NA	NA	W	Troubleshooting user/system issues
System Admin	A	NA	A	NA	A	A	Infrastructure management (No finance access)
Intern	W	NA	NA	NA	L	W	Restricted access to assigned resources
Contractor	W	L	NA	NA	NA	L	Time-bound scoped access

Administrators

The following individuals have administrative privileges for critical systems:

- **Mary Wairimu:** All Systems (System Admin)
- **Mark Shah:** GitHub & Infrastructure (DevOps Admin)
- **Susan Wangari:** Finance System (Finance Admin)
- **Rachel Atieno:** Security Monitoring Tools (Security Admin)

Exceptions / Special Access

Note: The following exceptions to standard access control rules exist within the organization.

- DevOps Engineers may request **temporary production access** via JIT approval.
- External auditors may receive **time-bound read-only access** during audits.
- Contractors are granted **expiry-based access** tied to contract duration.
- Emergency access may be granted under **break-glass procedures**, subject to audit.

Access Review Logs

Access rights should be reviewed periodically. The table below logs the most recent access reviews.

Review Date	Reviewed By	Findings
3/31/2026	Security Team	No orphaned accounts found
1/1/2026	IT Admin	Overprovisioned finance access corrected

Approval

This document has been reviewed and approved by the following personnel:

- James Mwangi – CEO (Approved on: 2026-04-01)
- Rachel Atieno – Security Lead (Approved on: 2026-04-01)
- David Kim – CTO (Approved on: 2026-04-01)