NOVATECH SOLUTIONS · SIMULATED ENTERPRISE ENVIRONMENT

# Enterprise Identity & **Access Governance System**

Project Documentation · Identity & Access Management Division

RBAC | MFA Enforcement | JML Lifecycle | Zero Trust | Privileged Access | Audit Logging

| VERSION | CLASSIFICATION | DIVISION | ORGANIZATION |
|---|---|---|---|
| 2.0 | Confidential — Internal Use | Identity & Access Management | NovaTech Solutions |

## 1 EXECUTIVE SUMMARY

This document presents the design and implementation specification of a centralized Identity and Access Management (IAM) governance framework for NovaTech Solutions, a simulated mid-sized technology company operating cloud-hosted internal systems across HR, Finance, Engineering, and Customer platforms.

The framework enforces least-privilege access, reduces privilege sprawl, and provides structured identity lifecycle control across all enterprise systems. It integrates the following core controls:

**Role-Based Access Control (RBAC)**
Centrally enforced — no direct user permissions

**Multi-Factor Authentication (MFA)**
Mandatory for all users and systems

**JML Lifecycle Automation**
Structured provisioning and revocation

**Just-In-Time (JIT) Privileged Access**
Time-bound, approval-gated escalation

**Centralized Audit Logging**
Full traceability aligned to SIEM

**Zero Trust Architecture**
No implicit trust — every request verified

> **Key Security Principle:** All access is role-based and centrally enforced — no direct user permissions exist. Every identity action is logged and traceable.

## 2 SECURITY OBJECTIVES

The IAM governance model is designed to achieve the following security objectives, aligned with ISO 27001-style principles:

**Prevent Unauthorized Access**
Enforce authentication barriers at every system entry point

**Enforce Least Privilege at Scale**
Grant only the minimum permissions required for each role

**Reduce Insider Threat Risk**
Limit the blast radius of compromised or misused accounts

**Ensure Traceable Identity Actions**
Maintain complete audit trails for all access events

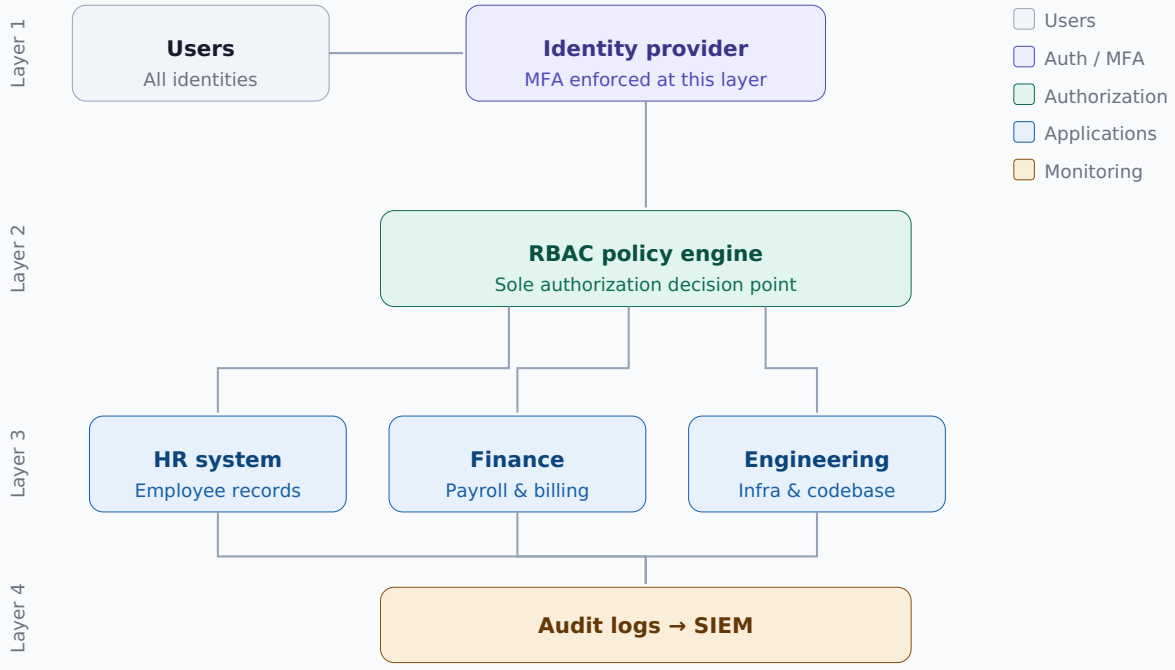
**Support Audit and Compliance**
Align with ISO 27001-style controls and documentation standards

**Standardize Access Across Depts**
Apply consistent policies across all business units

## 3 IAM ARCHITECTURE

The IAM architecture implements a layered security model that separates authentication from authorization. All identity flows pass through a centralized policy decision point before reaching any enterprise system.

DIAGRAM 1 — IAM ARCHITECTURE: END-TO-END IDENTITY FLOW




**Layer 1 — Authentication:** All users authenticate through the central Identity Provider before any authorization decision is made. MFA is enforced at this layer for every user.

**Layer 2 — Authorization:** The RBAC Policy Engine is the sole decision point. It evaluates the authenticated user's role and grants or denies access. No direct user-to-permission bindings exist.

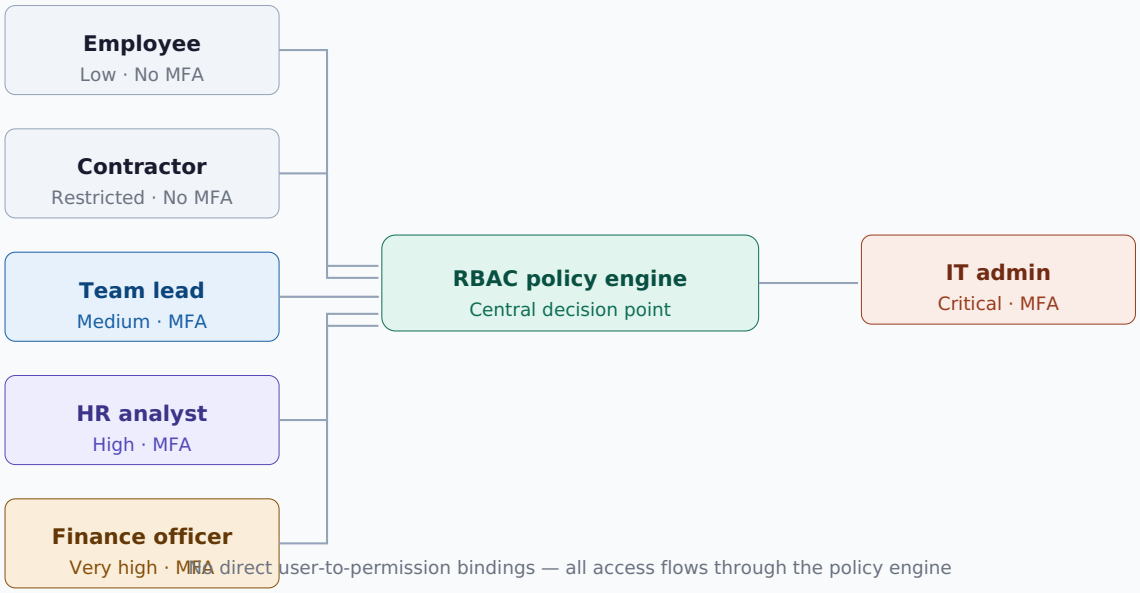
**Layer 3 — Applications:** HR, Finance, Engineering, and Customer platforms receive access tokens from the policy engine. They do not manage their own access control logic.

**Layer 4 — Audit & Monitoring:** All access events are forwarded to centralized audit logging and SIEM for real-time visibility and compliance evidence.

## 4 ROLE-BASED ACCESS CONTROL (RBAC) MODEL

The RBAC model defines a clean, scalable role hierarchy where every access decision flows through an assigned role. No user is granted permissions directly. This ensures consistency, auditability, and minimal privilege sprawl.

DIAGRAM 2 — RBAC ROLE HIERARCHY & PERMISSION TIERS

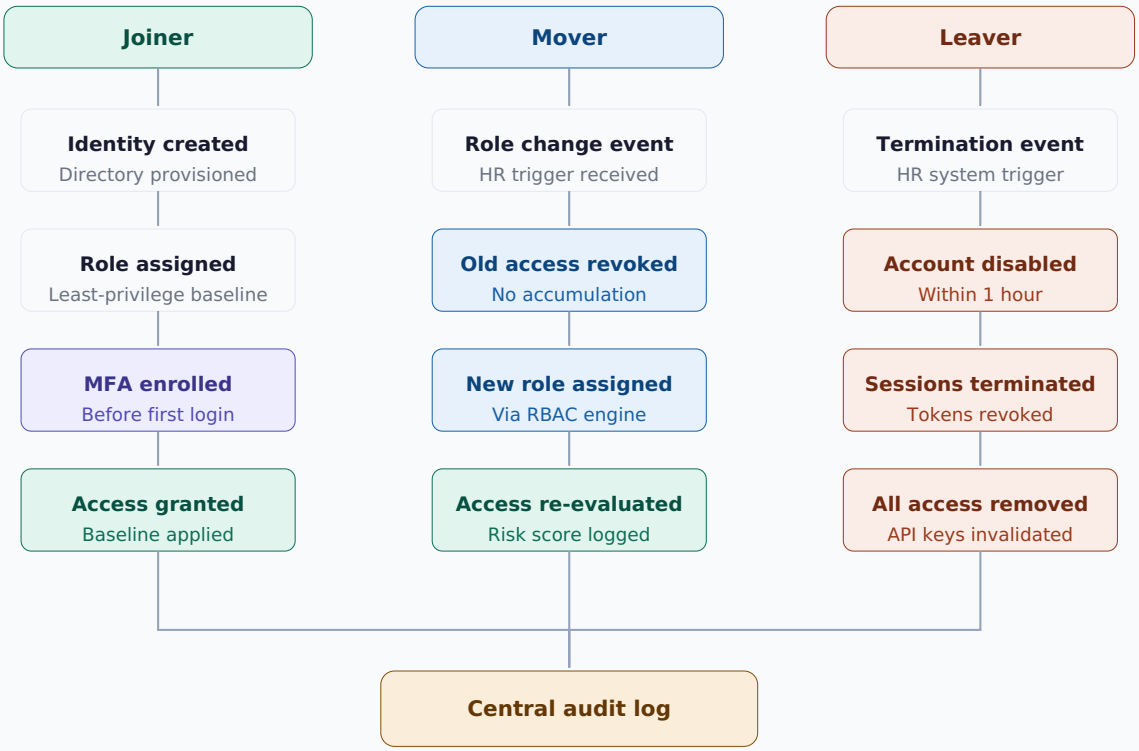



| Role | Access Scope | Security Level | MFA Required |
|---|---|---|---|
| Employee | Email, Docs, Internal Portal | Low | No |
| Contractor | Single Project Access Only | Restricted | No |
| Team Lead | Team Reports, Project Data | Medium | Yes |
| HR Analyst | HR Records System | High | Yes |
| Finance Officer | Payroll + Billing Systems | Very High | Yes |
| IT Admin | Infrastructure + IAM Controls | Critical | Yes |

## 5 JOINER-MOVER-LEAVER (JML) LIFECYCLE

The JML lifecycle model governs how user identities and access rights are managed throughout the employment lifecycle. Each stage has defined procedures, automated controls, and audit requirements.

DIAGRAM 3 — JML IDENTITY LIFECYCLE FLOWCHART




**5.1 Joiner — Day 0 Access Provisioning:** Identity created in central directory → least-privilege role assigned → MFA enforced before first login → baseline access applied → audit logging active from account creation.

**5.2 Mover — Role Transition Control:** Previous permissions fully revoked with no accumulation → new role assigned through RBAC engine → access re-evaluated automatically → risk score and change event recorded.

> **5.3 Leaver — Offboarding Security:** All leaver actions must be completed within one hour of the termination event being recorded. Account disablement, session termination, token revocation, and API key invalidation are automated. The audit trail is preserved in read-only state for compliance retention.

## 6 PRIVILEGED ACCESS MANAGEMENT

Privileged access is never permanent. All elevated access is governed by a Just-In-Time (JIT) workflow that requires explicit justification, approval, and automatic time-bound revocation, reflecting Zero Trust security principles.

1. **Access Request:** User submits a request for elevated privileges with business justification.
2. **Manager Approval:** Direct manager reviews and approves or denies the request.
3. **Security Validation:** Security team validates the justification against current risk posture.
4. **Time-Bound Grant:** Temporary elevated role assigned with a defined expiry window.
5. **Automatic Revocation:** Access automatically removed at expiry — no manual action required.
6. **Audit Retention:** Full log of the request, approval, usage, and revocation retained.

> **Zero Trust Alignment:** No standing privileges, every access request is verified, and access is granted for the minimum time required to complete the task.

## 7 MFA ENFORCEMENT POLICY

Multi-Factor Authentication is mandatory for all users across the NovaTech environment, with additional controls for high-risk roles and access scenarios.

| Scope | MFA Requirement |
|---|---|
| All user accounts | Mandatory without exception |
| All administrative roles | Mandatory — IT Admin, Security Team |
| All Finance system access | Mandatory — Payroll, Billing, Ledger |
| All remote access and VPN | Mandatory |
| All JIT privilege escalations | Mandatory at each escalation event |

MFA must be enrolled before the first system login. Repeated MFA failures trigger account lockout. MFA bypass is not permitted under any operational circumstances.

## 8 CONTRACTOR ACCESS CONTROL

Contractor accounts are subject to stricter controls than permanent employee accounts, reflecting the elevated risk of third-party access to enterprise systems.

| Control | Policy |
|---|---|
| Account duration | 30-day default — no grace period on expiry |
| Access scope | Assigned project only — no cross-project access |
| Administrative rights | Not granted under any circumstances |
| Access extension | Formal re-validation and approval required |
| Audit logging | Enhanced logging applied to all contractor activity |

> Extensions beyond 30 days must be submitted at least 5 business days prior to expiry and are subject to the same JIT approval workflow as privileged access requests.

## 9 AUDIT AND MONITORING STRATEGY

The centralized audit logging strategy ensures complete visibility across all identity and access events. Logs are retained in a tamper-resistant format and feed into security monitoring for real-time threat detection and compliance reporting.

| Event Type | Description | Triggered By | Frequency |
|---|---|---|---|
| Authentication attempts | Identity verification activity | All users | Real-time |
| MFA failures | Failed second-factor challenges | All users | Real-time |
| Role changes | Permission updates and assignments | Managers, IT | On change |
| Privilege escalation | JIT access requests and approvals | IT Admin | On change |
| System access logs | Resource access per application | All users | Continuous |
| Admin actions | Configuration and policy changes | IT Admin | Real-time |

## A APPENDIX — KEY SECURITY PRINCIPLES

**Least Privilege Access**
Users and systems are granted only the minimum permissions required to perform their function.

**Role-Based Access Control**
All permissions are assigned via roles — no direct user-to-resource bindings exist.

**Multi-Factor Authentication**
Every authentication event requires a second factor, regardless of role or location.

**Zero Trust Security**
No implicit trust is granted to any user, device, or network — every request is verified.

**Centralized Audit Logging**
All identity events are recorded centrally for traceability, investigation, and compliance.

**Privileged Access Management**
Elevated access is time-bound, approval-gated, and automatically revoked on expiry.