Zero Trust Access Control

Least Privilege • MFA • Identity Governance

Zero Trust	RBAC	MFA	IAM Concepts

Overview

This case study demonstrates how EPIC TECH LLC approaches access control using least privilege, role-based access, MFA, logging, and access revocation principles.

Business Challenge

Businesses can expose sensitive systems when employees, contractors, or vendors have broad or outdated permissions. Access should be approved, limited, monitored, and removed when no longer needed.

Example Solution

A structured access enforcement model was documented using authorization workflows, role-based access concepts, MFA, audit logging, and immediate revocation expectations.

Technologies / Methods Demonstrated

- Zero Trust
- RBAC
- MFA
- IAM Concepts
- Access Reviews
- Audit Logging
- Vendor Access Control

Business Outcomes

- Reduced unnecessary access.
- Improved accountability for sensitive systems.
- Created a repeatable access governance model for business environments.

What This Shows a Client

- Shows identity and access control understanding.
- Shows policy-to-technical-control thinking.
- Shows focus on least privilege and auditability.

Details intentionally not published

- Full internal policy templates.
- Exact access groups and role maps.

- Client-specific workflow approvals.
- Internal audit log structure.

This document is designed to give website visitors confidence in EPIC TECH LLC capability without publishing full implementation playbooks or reusable client deliverables.