Security Policy Gap Analysis (NIST CSF)

Problem Statement

Many organizations maintain security policies that are not fully aligned with industry frameworks, leading to gaps in governance and enforcement. This project evaluates existing policies against the NIST Cybersecurity Framework to identify gaps and recommend improvements.

Policies Reviewed

- Access Control Policy
- Acceptable Use Policy

Framework Used

NIST Cybersecurity Framework (CSF)

Methodology

Reviewed policy language, mapped controls to NIST CSF categories, identified gaps, assessed risk impact, and proposed policy enhancements.

Key Findings

Policies lacked explicit enforcement language, MFA requirements were unclear, and accountability was insufficiently defined.

Recommendations

Update policies to mandate MFA, clarify roles and responsibilities, and align language with NIST CSF standards.

Outcome

Improved policy alignment, stronger governance structure, and reduced compliance and access-related risk.