Security Policy Development and Enforcement

Prepared by: Leo D. Dorsey

Objective

To create, document, and implement security policies that support organizational security goals, meet compliance standards, and improve user behavior across the organization.

Tools & Methods

Tools Used: Microsoft Word, Google Docs, internal wiki system, PDF export

References: NIST SP 800-53, CIS Controls, ISO/IEC 27002

Deliverables:

- Acceptable Use Policy
- Password Policy
- Access Control Policy
- Remote Work & BYOD Policy

Implementation Steps

1. Conducted internal interviews to identify policy gaps
2. Researched compliance standards and peer organizations
3. Drafted plain-language, enforceable policies tailored to the environment
4. Collaborated with IT and HR for review and approval
5. Published policies and tracked user acknowledgment
6. Developed periodic review schedule and version control

Results / Findings

- All employees signed Acceptable Use and BYOD policy by deployment week
- Reduced helpdesk tickets related to password resets by 30%
- Improved awareness of security roles and responsibilities

- Policies integrated into onboarding and quarterly reviews

Conclusion

This project strengthened the organizations security posture through clearly documented, widely adopted policies. It bridged the gap between technical controls and human behavior, while laying the groundwork for future audits and compliance efforts.