**Task-2**

**Security Policy Review and Enhancement**

**1. Access Control Policy:**

- Current State:

- User accounts exist but lack strong password requirements.

- No implementation of two-factor authentication (2FA).

- Gaps Identified:

- Passwords are weak and not regularly updated.

- Lack of multi-factor authentication leaves systems vulnerable.

**2. Data Protection Policy:**

- Current State:

- Backups are performed manually weekly.

- Data encryption policies are inconsistent.

- Gaps Identified:

- No real-time automated backup system.

- Only partial implementation of encryption.

**3. Incident Response Policy:**

- Current State:

- Incidents are logged but lack a structured response procedure.

- Gaps Identified:

- No post-incident review or reporting.

- Employees are not trained on incident response.

**II. Identified Improvements**

**1. Access Control:**

- NIST Recommendations:

- Implement strong password policies: at least 12 characters, including uppercase, lowercase, numbers, and special symbols.

- Make 2FA mandatory across all user accounts.

- Example Update:

- "Passwords must be changed every 90 days, and accounts without 2FA will be disabled."

**2. Data Protection:**

- ISO/IEC 27001 Recommendations:

- Automate backup processes with real-time synchronization.

- Encrypt all sensitive data using AES-256 encryption.

- Example Update:

- "All sensitive files must be stored on encrypted drives, with backups synchronized daily to a secure server."

**3. Incident Response:**

- SANS Best Practices:

- Develop Standard Operating Procedures (SOPs) for incident handling.

- Perform a root cause analysis after each incident.

- Example Update:

- "Establish a dedicated incident response team to monitor and manage cybersecurity events."

**III. Example of Updated Policy Document**

Access Control Policy

**Approved By**: [Organization Name] Security Team

**Date:**November 15, 2024

**Policy ID**: AC-01

**1. Purpose:**

- To ensure the security of organizational data and systems by standardizing access controls.

**2. Policy:**

- Users must access only the resources required for their roles.

- Passwords must:

- Be at least 12 characters long.

- Include uppercase, lowercase, numbers, and special characters.

- All accounts must have 2FA enabled.

**3. Responsibilities:**

- Security Manager: Oversees policy enforcement.

- IT Department: Implements user access controls.

**4. Non-Compliance:**

- Accounts violating this policy will be deactivated until rectified.

**IV. Implementation Plan**

**1. Training and Awareness:**

- Organize training sessions for employees on updated policies.

- Use workshops to demonstrate the importance of strong passwords and 2FA.

**2. Monitor Compliance:**

- Perform regular audits to ensure all policies are followed.

- Use automated tools to monitor for potential policy violations.

**3. Continuous Improvement:**

- Gather feedback from employees and stakeholders to refine policies further.

- Regularly update policies to address emerging threats and align with standards.