3.4 Design a network security policy for a small organisation.

1. Objectives

Confidentiality – To protect information and the organization's data.

Integrity – To ensure the data is authenticated and reliable.

Availability – Guarantee the availability of network services and resources at all times.

Risk Management – Identify, assess, and mitigate network security risks.

Compliance – Meet legal, regulatory, and contractual obligations.

2. **Scope**

Includes all network infrastructure, wired and wireless networks.

All devices connected to the network including servers, end devices, network devices, workstations.

Apply the policy to all employees and third-party users with access to the organization's network resources.

3.**Responsibilities**

IT Department – Implement and manage network security measures. Conduct regular audits, and respond to security incidents.

Employees and Users – Adhere to the security policy. Report any security incidents. Participate in training programs.

4.**Access Control**

User Authentication – Authenticate users using strong passwords and multi-factor authentication.

Role-Based Access Control (RBAC) – Limit access to network resources and organization's data based on job roles. Ensure the principle of least privilege.

Account Management – Create user accounts, manage and deactivate them. Do regular reviews to ensure inactive accounts are removed.

5.**Network Security**

Firewalls – implement and configure firewalls to protect the network from unauthorized access and threats.

Password protection – enforce strong password policies, including password changes and complexity password requirements.

Network monitoring – Use intrusion detection and prevention systems (IDS/IPS) to monitor network traffic and detect anomalies.

6.**Data Protection**

Encryption – Encrypt sensitive data using industry standard encryption protocols.

Backup – Regularly backup critical data and configurations, and store backups securely. Test backup integrity periodically.

7.**Email and Internet Use**

Acceptable Use Policy (AUP) – Define permissible activities for email and internet use. Prohibit the use of personal email accounts for work purposes, the use of work email accounts for personal cases, and accessing inappropriate, unsecure websites.

8. **Physical Security**

Physical access control – restrict physical access to network infrastructure and sensitive areas to authorized personal only.

Biometric security – Use fingerprint and facial recognition systems for secure access to critical areas and devices.

Surveillance – Implement surveillance cameras and monitor sensitive areas.

9.**Incident Response**

Report all security incidents immediately to the IT department. Develop and maintain an incident response plan. Conduct forensic analysis.

10.**Training for employees**

Conduct security awareness training to employees to educate on security practices, social engineering attacks, and new threats. Perform policy training to ensure all employees familiar with the network security policy and their responsibility.