Security Documentation Deliverables

1. Security Control Implementation: FileVault Encryption (macOS)

Objective:

Implement full disk encryption using FileVault to protect data at rest.

System Requirements:

- macOS 11 or later
- Admin privileges

Steps:

1. Go to System Settings > Privacy & Security > FileVault
2. Click 'Turn On FileVault'
3. Choose recovery method (iCloud or local key)
4. Reboot to begin encryption

Verification:

Run 'fdesetup status' to confirm FileVault is enabled.

Security Impact:

- Protects sensitive data on lost or stolen devices
- Supports compliance (ISO 27001 A.10.1)

2. Step-by-Step Guide: Linux Patch Management

1. Run update check:

```
sudo apt update
```

2. List available patches:

```
apt list --upgradable
```

3. Apply patches:

```
sudo apt upgrade -y
```

4. Reboot if required:

   sudo reboot

5. Check logs at:

   /var/log/apt/history.log

3. Incident Response Playbook: Malware Infection

Trigger: Malware alert or suspicious file activity

Steps:

- Isolate affected host from the network
- Create forensic image or use log2timeline for timeline analysis
- Remove malicious files or reimage system
- Document actions taken and file hashes
- Monitor system after restoration

4. Incident Response Playbook: Phishing Attempt

Trigger: User reports suspicious email

Steps:

- Analyze email headers for spoofing
- Block sender domain in email system
- Search for similar emails across users
- Reset credentials if credentials were submitted
- Notify all users with a phishing alert

5. Structured Document Repository

Example Directory Structure:

Security Documentation Deliverables

/KB/

- Security_Control_Implementations/
  - FullDiskEncryption_FileVault.md
- Guides/
  - Patch_Management_Guide.md
- Playbooks/
  - Malware_Response_Playbook.md
  - Phishing_Response_Playbook.md
- Templates/
  - ChainOfCustody_Form.md