#### Week 1: Onboarding and Training

Step 1: Attend Initial Training Session

1. Schedule and Attend Training
   * Check your email for the training session schedule.
   * Attend the session on time and actively participate.
2. Learn Cybersecurity Principles
   * Pay attention to the basics of cybersecurity, including confidentiality, integrity, and availability.
   * Take notes on key concepts and tools introduced.
3. Review Resources and Templates
   * Access the provided resources and templates from the shared drive or learning platform.
   * Familiarize yourself with these materials, as they will be used throughout the internship.

#### Week 2: Security Basics

Step 2: Introduction to Cyber Threats

1. Research Cyber Threats
   * Use reliable sources such as cybersecurity blogs, articles, and official documentation to research common threats like malware, phishing, and ransomware.
2. Create a Summary Report
   * Summarize each threat, including what it is, how it works, and its impact on organizations.
   * Use a word processor to compile your findings into a clear, concise report.
3. Submit the Report
   * Share your report with your mentor for feedback via email or the designated submission platform.

Step 3: Password Security

1. Research Password Security
   * Study articles and guidelines on the importance of strong passwords and best practices for password management.
2. Develop Guidelines
   * Create a set of guidelines for creating and managing strong passwords. Include examples and tips.
3. Create a Short Document
   * Use a word processor to write a document presenting your guidelines.
4. Submit for Feedback
   * Share the document with your mentor for review and suggestions.

#### Week 3: Network Security

Step 4: Network Vulnerability Assessment

1. Learn to Use Tools
   * Watch tutorials or read guides on how to use tools like Nmap or Wireshark for network scanning.
2. Conduct an Assessment
   * Use Nmap to scan a network for open ports and services.
   * Use Wireshark to capture and analyze network traffic.
3. Identify Vulnerabilities
   * Note any vulnerabilities or security issues found during your scans.
4. Summarize Findings
   * Write a report detailing the vulnerabilities found and recommended actions to address them.
5. Submit the Report
   * Share your report with your mentor for feedback.

Step 5: Firewall Configuration

1. Learn Firewall Basics
   * Study basic concepts and configurations of firewalls through online resources or tutorials.
2. Create a Simple Guide
   * Write a step-by-step guide on configuring a basic firewall for a local network, using screenshots or illustrations to aid understanding.
3. Submit the Guide
   * Share the guide with your mentor for review.

#### Week 4: Data Security

Step 6: Data Encryption

1. Research Data Encryption
   * Learn about the importance of encryption and different encryption methods by reading articles and watching videos.
2. Create a Tutorial
   * Write a simple tutorial on how to encrypt files using tools like VeraCrypt or BitLocker. Include screenshots and detailed steps.
3. Submit the Tutorial
   * Share the tutorial with your mentor for feedback.

Step 7: Backup Strategies

1. Investigate Backup Strategies
   * Research different types of data backup strategies and their advantages.
2. Develop a Backup Plan
   * Create a basic backup plan for a small organization, specifying the frequency and type of backups.
3. Present the Backup Plan
   * Write a report detailing the backup plan and submit it for review.

#### Week 5: Incident Response

Step 8: Incident Response Plan

1. Research Incident Response Plans
   * Study the components and best practices for incident response plans through articles and case studies.
2. Develop a Template
   * Create a basic template for an incident response plan, outlining steps for identifying, containing, eradicating, and recovering from incidents.
3. Present the Plan
   * Write a detailed document based on the template and submit it for review.