Day 1: Security Fundamentals and Data Protection

1. **Introduction to Security**
   - Overview of Security in the Digital Age
   - The Importance of Data Protection
2. **Threat Landscape**
   - Understanding Modern Threats
   - Common Cybersecurity Risks
3. **Data Classification and Handling**
   - Identifying Sensitive Data
   - Best Practices for Data Classification
4. **Data Encryption**
   - Basics of Data Encryption
   - Encryption Techniques and Algorithms
5. **Access Control**
   - Role-Based Access Control
   - Implementing Access Control Policies
6. **Security Awareness**
   - Building a Security-Aware Culture
   - Employee Training and Awareness Programs

Day 2: Risk Management and Compliance

7. **Risk Assessment**
   - Identifying and Assessing Risks
   - Risk Assessment Methodologies
8. **Security Policies and Procedures**
   - Developing Security Policies
   - Establishing Security Procedures
9. **Incident Response and Recovery**
   - Incident Handling and Reporting
   - Recovery Strategies and Planning
10. **Compliance and Regulations**
    - Overview of Security Regulations
    - Achieving Compliance
11. **Security Technologies**
    - Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS)
    - Endpoint Security Solutions
12. **Security Best Practices**
    - Security in the Cloud

- Mobile Device Security

13. **Course Review and Q&A**
    - Recap of Key Concepts
    - Questions and Answers