Enterprise Security Plan Final Paper Contents Guideline

I. Introduction
   a. Scope of Information Security Management
   b. Impact of Security Breaches
   c. Common Attacks
   d. Defense in Depth Strategy
   e. Enterprise Security Plan Sponsor

II. Enterprise Security Policy Plan
   a. Security Governance
   b. Security Control Framework Selection
   c. Maintaining the Security Policy Portfolio
   d. Enterprise Risk Management
   e. Different Policy Audiences

III. Enterprise Technical Infrastructure Security Plan
   a. Network and Host Firewalls
   b. Network-based Intrusion Detection and Prevention
   c. Host-based Intrusion Prevention
   d. Network and Host Monitoring
   e. Infrastructure Change, Configuration and Patch Control

IV. Enterprise Risk Assessment Plan
   a. Administrative, Technical and Physical Controls
   b. Risk Analysis and Treatment
   c. Risk Scoring Approach

V. Enterprise Policy for Auditing Plan
   a. Ethical Hacking
   b. Auditing versus Assessment Approach
   c. Financial versus Security Audits

VI. Cyberlaw Policy Plan
   a. Regulatory Policy to Organization Mapping
   b. Organizational Policy Alignment
   c. Cyberlaw Enforcement

VII. Enterprise Business Continuity and Disaster Recovery Strategy Plan
   a. Information Retention Schedule
   b. Business Impact Assessment (BIA)
   c. Critical Infrastructure and Assets
   d. Sponsorship for BCP and DRP Testing

VIII. Enterprise Security Awareness Training Organizational Strategy Plan
   a. Information Leakage and Insider Threats
   b. Security Awareness Training Acknowledgement
   c. Frequency of Security Awareness Training

IX. Enterprise Organizational Policy for Identity Management Plan
   a. Enterprise and Mobile Authentication
   b. Enterprise and Remote Authorization (Access Control)
   c. Centralized and Federated Identity Management

- X. Enterprise Incident Response, CSIRT and Forensics Plan
    - a. Incident Life Cycle
    - b. Responding to Incidents with CSIRT
    - c. Network Forensics
    - d. Digital Forensics-based Investigation and Lab Operations
- XI. Enterprise Penetration (Pen) Testing Plan
    - a. Types of Pen Testing
    - b. Pen Testing Methodology
    - c. Legal Consequence
- XII. Enterprise Information Security Implementation Plan
    - a. Physical Security
    - b. Authentication
    - c. Network Security
    - d. Encryption
    - e. Software Development
    - f. Email
    - g. Internet
    - h. Acceptable Use
    - i. Disaster Recover
    - j. Business Continuity
    - k. Security Awareness
    - l. Viruses/Worms
- XIII. Conclusion
- XIV. References (APA Style Guide Format)
- XV. Appendices