TABLE OF CONTENTS

Chapter 1: Introduction to DevSecOps and Secure Engineering **01-15**

1.1 Evolution from DevOps to DevSecOps
1.2 Principles of "Shift Left" Security
1.3 Importance of Security in Regulated Environments
1.4 Overview of Secure Software Development Lifecycle (SSDLC)
1.5 Challenges and Opportunities in Modern Secure Systems

Chapter 2: Regulatory Frameworks and Compliance Requirements **16-30**

2.1 Overview of Global Regulations (GDPR, HIPAA, ISO 27001, etc.)
2.2 Industry-Specific Compliance Standards
2.3 Risk Management and Governance Models
2.4 Data Privacy and Protection Principles
2.5 Compliance Automation in DevSecOps

Chapter 3: DevSecOps Architecture and Toolchain **31-48**

3.1 CI/CD Pipeline Security Integration
3.2 Secure Code Repositories and Version Control
3.3 Static and Dynamic Application Security Testing (SAST & DAST)
3.4 Container Security and Orchestration (Docker, Kubernetes)
3.5 Infrastructure as Code (IaC) Security

Chapter 4: Agentic AI in Secure Development **49-64**

4.1 Introduction to Agentic AI Systems
4.2 AI-Driven Threat Detection and Response
4.3 Autonomous Security Testing and Code Review
4.4 Risks and Ethical Considerations of AI in Security
4.5 Integration of AI Agents in DevSecOps Pipelines

Chapter 5: Secure Data Pipelines and Data Engineering **65-85**

5.1 Data Pipeline Architecture and Components
5.2 Data Encryption and Secure Transmission
5.3 Data Integrity and Validation Techniques
5.4 Secure Data Storage and Access Control
5.5 Monitoring and Auditing Data Pipelines

Chapter 6: Threat Modeling and Risk Assessment **86-111**

6.1 Fundamentals of Threat Modeling (STRIDE, DREAD)
6.2 Vulnerability Assessment Techniques
6.3 Risk Analysis and Mitigation Strategies
6.4 Security Testing Frameworks and Tools
6.5 Continuous Risk Monitoring in Pipelines

Chapter 7: Scaling Security in Cloud and Distributed Systems **112-138**

7.1 Cloud Security Models (IaaS, PaaS, SaaS)
7.2 Multi-Cloud and Hybrid Cloud Security
7.3 Zero Trust Architecture Principles
7.4 Identity and Access Management (IAM)
7.5 Scalability Challenges and Solutions in Secure Systems

Chapter 8: Future Trends and Best Practices **139-171**

8.1 Emerging Trends in DevSecOps and AI Security
8.2 Best Practices for Secure Software Delivery
8.3 Continuous Compliance and Monitoring
8.4 Case Studies in Regulated Environments
8.5 Roadmap for Implementing Scalable Secure Systems