Cybersecurity Policy Development Training Course

Professional Development Training Course Outline

Category	Criminology	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

As cyber threats continue to grow in complexity and frequency, it is critical for organizations to develop robust cybersecurity policies that are both adaptive and proactive. Training Course on Cybersecurity Policy Development is designed to equip IT professionals, decision-makers, and cybersecurity leaders with the skills and insights required to create, implement, and maintain security policies aligned with international standards, legal requirements, and real-world threats. The course integrates hands-on policy creation with current threat intelligence, governance models, and compliance frameworks.

With an emphasis on risk management, regulatory compliance, incident response, and policy lifecycle management, participants will master the essential components that protect digital infrastructures. Attendees will also gain access to case-based learning, policy frameworks, and strategic implementation techniques to ensure operational resilience and digital trust in the face of evolving cyber challenges.

Programme Curriculum

Cybersecurity Policy Development Training Course

Introduction

As cyber threats continue to grow in complexity and frequency, it is critical for organizations to develop robust cybersecurity policies that are both adaptive and proactive. Cybersecurity Policy Development Training Course is designed to equip IT professionals, decision-makers, and cybersecurity leaders with the skills and insights required to create, implement, and maintain security policies aligned with international standards, legal requirements, and real-world threats. The course integrates hands-on policy creation with current threat intelligence, governance models, and compliance frameworks.

With an emphasis on risk management, regulatory compliance, incident response, and policy lifecycle management, participants will master the essential components that protect digital infrastructures. Attendees will also gain access to case-based learning, policy frameworks, and strategic implementation techniques to ensure operational resilience and

digital trust in the face of evolving cyber challenges.

Training Objectives

1. Understand the fundamentals of cybersecurity governance and policy frameworks.
2. Analyze cyber risk management strategies within enterprise environments.
3. Develop comprehensive information security policies tailored to organizational needs.
4. Integrate compliance standards such as ISO 27001, NIST, and GDPR into policy creation.
5. Design incident response protocols aligned with modern threat landscapes.
6. Assess and mitigate insider threats and data breaches through policy design.
7. Utilize threat intelligence in policy decision-making processes.
8. Enhance cloud security policies and address third-party risks.
9. Implement access control and identity management policies.
10. Build cybersecurity awareness training policies for enterprise users.
11. Evaluate and update policies using policy audit frameworks.
12. Map cybersecurity policies to business continuity and disaster recovery plans.
13. Review real-world cybersecurity policy case studies for applied learning.

Target Audience

1. Chief Information Security Officers (CISOs)
2. Cybersecurity Managers and Analysts
3. IT Policy Makers and Strategists
4. Compliance Officers and Risk Managers
5. Government and Defense Personnel
6. Data Protection Officers (DPOs)
7. Legal and Regulatory Advisors
8. Technology Consultants and Auditors

Course Duration: 10 days

Course Modules

Module 1: Introduction to Cybersecurity Policy

- Definition and scope of cybersecurity policy
- Importance in organizational security posture
- Alignment with business objectives
- Stakeholder involvement in policy creation
- Overview of global policy standards
- **Case Study**: Google's policy evolution post-GDPR

Module 2: Cyber Risk Management Frameworks

- Risk identification and classification
- Risk analysis and quantification
- Control selection and evaluation
- Enterprise risk tolerance levels
- Residual risk and policy implications
- **Case Study**: JPMorgan’s $250M cybersecurity overhaul

Module 3: Policy Architecture and Governance Models

- Hierarchy of policies, standards, and procedures
- Governance and oversight structures

- Board involvement in cybersecurity strategy
- Policy version control and documentation
- Cybersecurity committees and roles
- **Case Study**: Governance at Microsoft Azure Security

Module 4: Compliance and Regulatory Integration

- Overview of ISO 27001/NIST/CIS controls
- Legal and industry compliance mandates
- Data privacy laws (GDPR, CCPA, HIPAA)
- Sector-specific compliance (financial, healthcare)
- Audit readiness and documentation practices
- **Case Study**: Meta’s response to global data laws

Module 5: Identity and Access Management Policies

- Principles of least privilege and segregation of duties
- Authentication, authorization, and accountability
- Single sign-on and multi-factor authentication
- Privileged Access Management (PAM)
- Role-based access control (RBAC)
- **Case Study**: Uber's insider breach due to IAM failure

Module 6: Cloud Security and Third-Party Risks

- Shared responsibility model in cloud computing
- Vendor risk management strategies
- Policy controls for SaaS, PaaS, IaaS
- SLAs and third-party audits
- Cloud encryption and data retention
- **Case Study**: Capital One AWS misconfiguration breach

Module 7: Data Protection and Classification Policies

- Data sensitivity and classification schemas
- Encryption standards and key management
- Secure data transfer protocols
- Data lifecycle policy creation
- Handling and retention requirements
- **Case Study**: Equifax’s failure in data classification

Module 8: Incident Response and Crisis Management

- Elements of an incident response policy
- Detection and triage mechanisms
- Roles and responsibilities in a crisis
- Communication and escalation protocols
- Forensics and root cause analysis
- **Case Study**: SolarWinds attack response breakdown

Module 9: Insider Threat Mitigation Policies

- Identifying insider threat vectors
- Behavioral monitoring and anomaly detection
- Least privilege enforcement
- Exit procedures and access revocation

- Whistleblower and reporting mechanisms
- **Case Study**: Edward Snowden and NSA policies

Module 10: Policy Communication and Training

- Organizational cybersecurity culture
- Training frameworks for staff
- Role-specific policy dissemination
- Policy onboarding and refresh cycles
- Feedback and continuous improvement
- **Case Study**: Boeing's employee security training

Module 11: Cybersecurity Audit and Policy Review

- Internal audit mechanisms
- Metrics for policy effectiveness
- Continuous monitoring and SIEM tools
- Policy gaps and remediation
- Audit documentation and follow-up
- **Case Study**: Target breach and policy audit failures

Module 12: Emerging Technologies and Policy Impact

- AI and machine learning in cybersecurity
- IoT device policy frameworks
- Blockchain-based security considerations
- Quantum computing readiness
- Ethical implications in tech policies
- **Case Study**: Tesla’s AI-enabled security systems

Module 13: Business Continuity and Disaster Recovery Policies

- BCP and DRP integration with security
- Recovery Point Objective (RPO) & Recovery Time Objective (RTO)
- Crisis simulations and tabletop exercises
- Policy role in minimizing downtime
- Lessons from ransomware incidents
- **Case Study**: Colonial Pipeline ransomware attack

Module 14: Policy Lifecycle Management

- Policy drafting, approval, and publication
- Change management and revision cycles
- Retention schedules and archival processes
- Version control best practices
- Retirement and end-of-life documentation
- **Case Study**: IBM’s evolving cybersecurity policy model

Module 15: Final Project – Policy Creation Simulation

- Team-based scenario policy development
- Application of real-world regulatory demands
- Integration of all modules into a cohesive document
- Presentation and peer review
- Instructor feedback and iteration
- **Case Study**: Simulated breach scenario and response plan

Training Methodology

- Instructor-led live sessions with Q&A
- Real-world policy document analysis
- Group discussions and peer collaboration
- Hands-on lab exercises and simulations
- Interactive policy creation workshops
- Quizzes and assessment at end of each module

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com