Training Course on Formulating ICT Security Policy

Professional Development Training Course Outline

Category	Information Technology	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s rapidly evolving digital landscape, cybersecurity threats have become more sophisticated and persistent. Organizations must implement robust ICT (Information and Communication Technology) security policies to safeguard sensitive data, ensure regulatory compliance, and protect critical infrastructure. Training Course on Formulating ICT Security Policy provides a comprehensive guide to formulating ICT security policies that align with modern frameworks, business goals, and legal obligations. With a focus on risk management, governance, and data protection, this training equips participants with practical strategies to build a secure digital environment.

As cyber-attacks, data breaches, and regulatory mandates increase, the need for enterprise-wide security policies is more urgent than ever. Participants will explore the critical components of effective ICT security policies, including access control, security architecture, compliance standards, and incident response planning. Designed for both technical and managerial professionals, this course emphasizes hands-on application and strategic development, ensuring participants can immediately implement best practices in their organizations.

Programme Curriculum

Training Course on Formulating ICT Security Policy

Introduction

In today’s rapidly evolving digital landscape, cybersecurity threats have become more sophisticated and persistent. Organizations must implement robust ICT (Information and Communication

Technology) security policies to safeguard sensitive data, ensure regulatory compliance, and protect critical infrastructure. Training Course on Formulating ICT Security Policy provides a comprehensive guide to formulating ICT security policies that align with modern frameworks, business goals, and legal obligations. With a focus on risk management, governance, and data protection, this training equips participants with practical strategies to build a secure digital environment.

As cyber-attacks, data breaches, and regulatory mandates increase, the need for enterprise-wide security policies is more urgent than ever. Participants will explore the critical components of effective ICT security policies, including access control, security architecture, compliance standards, and incident response planning. Designed for both technical and managerial professionals, this course emphasizes hands-on application and strategic development, ensuring participants can immediately implement best practices in their organizations.

Course Objectives

1. Understand the fundamentals of ICT security governance.
2. Identify current cybersecurity threats and vulnerabilities.
3. Analyze regulatory compliance requirements (GDPR, HIPAA, ISO 27001).
4. Design an effective risk management strategy.
5. Develop and implement a cybersecurity framework.
6. Define access control policies and authentication protocols.
7. Integrate network security and endpoint protection policies.
8. Draft an incident response and disaster recovery policy.
9. Monitor and audit ICT security policy performance.
10. Address cloud security and data privacy concerns.
11. Align ICT security with corporate governance policies.
12. Train staff in cyber hygiene and security awareness.
13. Develop documentation and policy review procedures using security best practices.

Target Audience

1. ICT Managers
2. Chief Information Security Officers (CISOs)
3. IT Governance Professionals
4. Network Security Engineers
5. Compliance Officers
6. Cybersecurity Analysts
7. Risk Managers
8. Policy and Strategy Advisors

Course Duration:

- 5 days

Course Modules

Module 1: Introduction to ICT Security Policy

- Importance of ICT security policy
- Key elements and definitions
- Cybersecurity ecosystem
- Security policy lifecycle
- Overview of legal and regulatory obligations

Module 2: Threat Landscape and Risk Assessment

- Understanding modern cyber threats
- Conducting risk assessments
- Vulnerability identification tools
- Business impact analysis
- Risk mitigation strategies

Module 3: Regulatory Compliance & Legal Frameworks

- GDPR, HIPAA, PCI-DSS, and ISO 27001
- Legal risks and penalties
- Policy alignment with compliance mandates
- Role of audits and inspections
- Industry-specific compliance cases

Module 4: Developing Security Policies

- Policy writing structure
- Roles and responsibilities definition
- Setting measurable objectives
- Cross-department collaboration
- Approval and rollout process

Module 5: Access Control & Authentication

- Defining user roles and permissions
- MFA (Multi-factor Authentication)
- Password policies and biometric solutions
- Identity management systems
- Privilege escalation controls

Module 6: Security Architecture & Technology Integration

- Security architecture layers
- Firewalls, IDS, and IPS policies
- Endpoint and network segmentation
- BYOD and remote access policies
- Cloud-based security models

Module 7: Incident Response & Disaster Recovery

- Incident response planning
- Recovery time objectives (RTOs)
- Forensic investigation guidelines
- Crisis communication strategies
- Post-incident policy revisions

Module 8: Training, Auditing, and Continuous Improvement

- Staff training programs
- Internal audits and monitoring
- Performance metrics
- Policy update cycles
- Feedback and improvement systems

Training Methodology

- **Interactive Workshops** – Scenario-based activities and simulations
- **Case Studies** – Real-world examples of ICT policy successes and failures
- **Expert Lectures** – Insight from industry leaders and practitioners
- **Hands-On Policy Writing** – Live exercises in formulating and reviewing policies
- **Assessment & Feedback** – Continuous evaluation through quizzes and peer reviews

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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