Training Course on Data Security and Technical Safeguards

Professional Development Training Course Outline

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

Course Introduction

In today’s hyperconnected digital era, data security and technical safeguards have become essential for protecting sensitive information across industries. Cyber threats, ransomware attacks, and unauthorized access have made it imperative for organizations to implement robust data protection measures. Training Course on Data Security and Technical Safeguards provides IT professionals, cybersecurity teams, and compliance officers with the skills and insights needed to manage data security risks, adopt best practices, and ensure regulatory compliance.

As regulations like GDPR, HIPAA, and CCPA grow stricter, the need for a deep understanding of access controls, data encryption, firewall management, and network security has never been greater. Participants in this course will explore the latest cybersecurity frameworks, tools, and real-world case studies to develop strategic solutions to modern security challenges.

Programme Curriculum

Training Course on Data Security and Technical Safeguards

Introduction

In today’s hyperconnected digital era, data security and technical safeguards have become essential for protecting sensitive information across industries. Cyber threats, ransomware attacks, and unauthorized access have made it imperative for organizations to implement robust data protection measures. Training Course on Data Security and Technical Safeguards provides IT professionals, cybersecurity teams, and compliance officers with the skills and insights needed to manage data security risks, adopt best practices, and ensure regulatory compliance.

As regulations like GDPR, HIPAA, and CCPA grow stricter, the need for a deep understanding of access controls, data encryption, firewall management, and network security has never been greater. Participants in this course will explore the latest cybersecurity frameworks, tools, and real-world case studies to develop strategic solutions to modern security challenges.

Course Objectives

1. Understand core principles of data security and cyber hygiene.
2. Identify and mitigate cybersecurity vulnerabilities in IT systems.
3. Apply technical safeguards like encryption and multi-factor authentication.
4. Comprehend compliance standards: HIPAA, GDPR, and ISO 27001.
5. Analyze real-world data breach case studies and lessons learned.
6. Implement endpoint security and cloud data protection protocols.
7. Manage access control and role-based permissions effectively.
8. Strengthen network perimeter defenses with firewalls and IDS/IPS.
9. Utilize risk assessment tools to evaluate information systems.
10. Explore emerging threats: AI-driven attacks and zero-day exploits.
11. Monitor and log data access with SIEM (Security Information & Event Management).
12. Create a cybersecurity incident response plan and escalation matrix.
13. Train staff in security awareness and phishing prevention techniques.

Target Audience

1. IT Security Professionals
2. Network Administrators
3. Compliance Officers
4. System Engineers
5. Data Protection Officers (DPOs)
6. Healthcare IT Managers (HIPAA-focused)
7. Cloud Security Consultants
8. Legal and Risk Analysts

Course Duration: 5 days

Course Modules

Module 1: Foundations of Data Security

- Introduction to data privacy principles
- Types of data threats and breaches
- Importance of confidentiality, integrity, and availability (CIA)
- Overview of cybersecurity frameworks (NIST, ISO)
- Legal regulations overview (GDPR, HIPAA)
- **Case Study**: Equifax Data Breach – Causes and Prevention Tactics

Module 2: Encryption & Cryptography Essentials

- Symmetric vs asymmetric encryption
- Role of PKI and SSL/TLS certificates
- Data-at-rest and data-in-transit protection
- Key management best practices
- Blockchain applications in data security
- **Case Study**: WhatsApp End-to-End Encryption Implementation

Module 3: Access Controls & Identity Management

- Role-based access control (RBAC)
- Multi-factor authentication (MFA) integration
- IAM tools and implementation
- Least privilege principle in organizations
- Managing user lifecycles securely
- **Case Study**: LinkedIn Credential Theft and IAM Gaps

Module 4: Network & Endpoint Security

- Network segmentation strategies
- Intrusion detection/prevention systems (IDS/IPS)
- Firewall configurations and use cases
- Endpoint detection and response (EDR)
- Securing mobile and IoT devices
- **Case Study**: Target POS Attack and Network Infiltration

Module 5: Cloud Security Safeguards

- Shared responsibility model in cloud
- Secure SaaS, IaaS, and PaaS models
- Cloud encryption and tokenization
- Cloud access security brokers (CASBs)
- Data residency and compliance in the cloud
- **Case Study**: Capital One AWS Misconfiguration Incident

Module 6: Data Loss Prevention (DLP) & Backup Strategies

- DLP tools and data classification
- Endpoint and network-based DLP
- Backup types: full, incremental, differential
- Offsite/cloud backup best practices
- Backup encryption and retention policies
- **Case Study**: Maersk Ransomware Attack and Recovery Strategy

Module 7: Incident Response & Forensics

- Phases of an incident response plan
- Cyber incident classification levels
- Digital forensics process and chain of custody
- Threat hunting and response automation
- Reporting and recovery metrics
- **Case Study**: SolarWinds Supply Chain Attack IR Tactics

Module 8: Security Awareness & Organizational Culture

- Building a security-first mindset
- Recognizing phishing and social engineering
- Periodic security training & simulation drills
- Employee data access audits
- Communication during security incidents
- **Case Study**: Twitter Employee Phishing and Insider Threats

Training Methodology

- Interactive lectures with expert-led discussions
- Live demonstrations of cybersecurity tools

- Real-world case study analysis
- Hands-on lab exercises and simulations
- Group activities and security scenario roleplays
- Post-training assessments and feedback review

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

Start Date	End Date	Location	Price
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