Training Course on Privacy Engineering and Secure Development Practices

Professional Development Training Course Outline

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

Course Introduction

In an era of increasing cyber threats and evolving data protection regulations, Privacy Engineering and Secure Development Practices are critical to safeguarding personal and organizational data. Training Course on Privacy Engineering and Secure Development Practices equips participants with the technical competencies, privacy frameworks, and secure coding standards necessary to build privacy-by-design applications. With a focus on real-world applications and threat modeling, learners will gain hands-on skills to engineer robust security measures from the ground up.

As data privacy becomes a cornerstone of digital trust, professionals in software development, cybersecurity, and IT compliance must stay ahead with proactive design techniques and secure development life cycle (SDLC) practices. This training merges the principles of GDPR, CCPA, and ISO/IEC 27701 with the latest in DevSecOps and zero-trust architecture, empowering teams to embed privacy in every layer of system development.

Programme Curriculum

Training Course on Privacy Engineering and Secure Development Practices

Introduction

In an era of increasing cyber threats and evolving data protection regulations, Privacy Engineering and Secure Development Practices are critical to safeguarding personal and organizational data. Training Course on Privacy Engineering and Secure Development Practices equips participants with the technical competencies, privacy frameworks, and secure coding standards necessary to build privacy-by-design applications. With a focus on real-world applications and threat modeling, learners will gain hands-on skills to engineer robust security measures from the ground up.

As data privacy becomes a cornerstone of digital trust, professionals in software development, cybersecurity, and IT compliance must stay ahead with proactive design techniques and secure development life cycle (SDLC) practices. This training merges the principles of GDPR, CCPA, and ISO/IEC 27701 with the latest in DevSecOps and zero-trust

architecture, empowering teams to embed privacy in every layer of system development.

Course Objectives

1. Understand the principles of privacy-by-design and privacy-by-default.
2. Apply secure coding practices across the software development lifecycle (SDLC).
3. Implement data minimization and encryption techniques.
4. Evaluate privacy risks using threat modeling and privacy impact assessments (PIAs).
5. Align development with GDPR, CCPA, and ISO 27001/27701 standards.
6. Integrate DevSecOps methodologies into agile and waterfall environments.
7. Develop automated privacy controls in CI/CD pipelines.
8. Use identity and access management (IAM) tools for secure authentication.
9. Build systems with zero trust architecture and least privilege access.
10. Conduct vulnerability scanning and penetration testing.
11. Document and manage consent and data subject rights in applications.
12. Create secure APIs using OWASP Top 10 best practices.
13. Analyze real-world data breaches and apply lessons in privacy engineering.

Target Audience

1. Software Developers
2. Security Engineers
3. IT Compliance Officers
4. DevOps Professionals
5. Privacy Officers
6. Risk Management Professionals
7. Product Managers
8. System Architects

Course Duration: 10 days

Course Modules

Module 1: Introduction to Privacy Engineering

- Definition and principles of privacy engineering
- Privacy-by-design vs. privacy-by-default
- Legal landscape (GDPR, CCPA, HIPAA)
- Privacy engineering lifecycle
- Role of privacy engineers in modern development
- **Case Study: Designing a mobile app with GDPR compliance**

Module 2: Secure Software Development Lifecycle (SDLC)

- Overview of secure SDLC phases
- Secure requirements engineering
- Security touchpoints in design, coding, and testing
- Integration of security in agile methodologies
- Tools for secure development
- **Case Study: SDLC enhancement for a fintech startup**

Module 3: Threat Modeling Techniques

- Introduction to STRIDE and LINDDUN
- Identifying data flows and attack surfaces

- Privacy threat categories
- Collaborative threat modeling workshops
- Risk prioritization frameworks
- **Case Study: Threat modeling in a healthcare app**

Module 4: Privacy Impact Assessments (PIA)

- Definition and legal requirements
- PIA process and templates
- Identifying stakeholders and data processors
- Mitigation strategies
- Documentation and audit readiness
- **Case Study: PIA implementation in a government e-service**

Module 5: Data Minimization and Anonymization

- Importance of data minimization
- Techniques for anonymization and pseudonymization
- Use of differential privacy
- Designing data retention policies
- Tools for automated data redaction
- **Case Study: Anonymizing customer analytics for a retail chain**

Module 6: Encryption Techniques and Key Management

- Symmetric vs. asymmetric encryption
- Best practices in key management
- Secure data-at-rest and in-transit
- Cryptographic protocols and libraries
- Encryption regulations and export controls
- **Case Study: Encrypting sensitive PII in cloud databases**

Module 7: Identity and Access Management (IAM)

- IAM frameworks and standards (OAuth, SAML, OpenID)
- Role-based access control (RBAC)
- Multi-factor authentication (MFA) integration
- IAM tools (Azure AD, Okta, Keycloak)
- Least privilege enforcement
- **Case Study: IAM overhaul for an e-commerce platform**

Module 8: Secure Coding Standards

- OWASP Top 10 vulnerabilities
- Secure coding in Java, Python, and JavaScript
- Input validation and output encoding
- Avoiding common cryptographic flaws
- Static code analysis tools
- **Case Study: Remediating insecure code in a legacy app**

Module 9: DevSecOps Integration

- CI/CD pipelines with security gates
- Container security with Docker and Kubernetes
- Infrastructure as Code (IaC) security
- DevSecOps toolchains (SonarQube, Checkmarx, GitHub Actions)

- Security testing automation
- **Case Study: Securing DevOps pipelines in a SaaS company**

Module 10: Secure API Development

- API security risks and protection
- OAuth 2.0 and API token strategies
- Input validation and rate limiting
- API gateways and WAFs
- API lifecycle and versioning controls
- **Case Study: Building secure REST APIs for banking apps**

Module 11: Privacy Governance and Compliance

- Overview of privacy governance frameworks
- Roles and responsibilities (DPO, CTO, CISO)
- Documentation and audit requirements
- Consent lifecycle management
- Vendor and third-party risk assessments
- **Case Study: Compliance readiness for a multinational enterprise**

Module 12: Secure Mobile and Web Development

- Security challenges in mobile apps
- Cross-platform vulnerabilities
- OWASP Mobile Top 10
- Secure session management
- Mobile app encryption
- **Case Study: Securing mobile access to corporate CRM**

Module 13: Incident Response and Breach Management

- Data breach lifecycle and reporting
- Role of the incident response team
- Coordination with legal and PR teams
- Breach containment and root cause analysis
- Legal obligations and penalties
- **Case Study: Incident response to a phishing attack in a hospital**

Module 14: Emerging Technologies and Privacy

- AI and machine learning privacy challenges
- IoT data security and compliance
- Blockchain and decentralized privacy models
- Cloud computing and shared responsibility
- Biometric data protection
- **Case Study: AI model privacy in a retail loyalty program**

Module 15: Final Capstone Project

- Design a secure application from scratch
- Conduct full threat modeling and PIA
- Develop security policies and controls
- Implement DevSecOps tools
- Present and defend privacy engineering decisions
- **Case Study: End-to-end privacy engineering for a health tech startup**

Training Methodology

- Interactive live instructor-led sessions
- Real-time hands-on lab simulations
- Use of tools: Burp Suite, OWASP ZAP, SonarQube
- Group discussions and peer reviews
- Project-based assessments and certification

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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