Data Masking and Tokenization Techniques Training Course

Professional Development Training Course Outline

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

Course Introduction

The proliferation of data, driven by digital transformation and cloud adoption, has made Data Security and Privacy Compliance non-negotiable business imperatives. Organizations routinely manage vast datasets containing Personally Identifiable Information (PII), Protected Health Information (PHI), and Payment Card Industry (PCI) data, creating significant regulatory and financial risk. Traditional security measures are often insufficient for protecting sensitive data used in Non-Production Environments like development, testing, and analytics.

Data Masking and Tokenization Techniques Training Course is engineered to bridge the critical gap between data utility and security. It provides in-depth, practical knowledge on two primary Data De-Identification techniques: Data Masking and Tokenization. By mastering these advanced methodologies, professionals can ensure Referential Integrity and Format Preservation while rendering sensitive data useless to unauthorized parties. Graduates will be equipped to implement a robust Data Privacy Framework that reduces breach risk, ensures continuous compliance with regulations like GDPR and HIPAA, and accelerates DevSecOps and Cloud Migration initiatives.

Programme Curriculum

Data Masking and Tokenization Techniques Training Course

Introduction

The proliferation of data, driven by digital transformation and cloud adoption, has made Data Security and Privacy Compliance non-negotiable business imperatives. Organizations routinely manage vast datasets containing Personally Identifiable Information (PII), Protected Health Information (PHI), and Payment Card Industry (PCI) data, creating significant regulatory and financial risk. Traditional security measures are often insufficient for protecting sensitive data used in Non-Production Environments like development, testing, and

analytics.

Data Masking and Tokenization Techniques Training Course is engineered to bridge the critical gap between data utility and security. It provides in-depth, practical knowledge on two primary Data De-Identification techniques: Data Masking and Tokenization. By mastering these advanced methodologies, professionals can ensure Referential Integrity and Format Preservation while rendering sensitive data useless to unauthorized parties. Graduates will be equipped to implement a robust Data Privacy Framework that reduces breach risk, ensures continuous compliance with regulations like GDPR and HIPAA, and accelerates DevSecOps and Cloud Migration initiatives.

Course Duration

5 days

Course Objectives

1. Master the foundational concepts of Data De-Identification, Anonymization, and Pseudonymization.
2. Differentiate between Static Data Masking (SDM) and Dynamic Data Masking (DDM) and their respective use cases.
3. Implement diverse Data Masking Techniques, including Shuffling, Substitution, Redaction, and Format-Preserving Encryption (FPE).
4. Design a Tokenization Strategy suitable for PCI DSS Compliance and secure payment processing.
5. Evaluate and select the appropriate data protection method (Masking vs. Tokenization) based on specific Data Utility and Reversibility requirements.
6. Apply a structured methodology for Sensitive Data Discovery and Data Classification across the enterprise.
7. Ensure Referential Integrity and Cross-System Consistency when masking complex relational databases.
8. Configure and manage a secure Token Vault and the associated De-Tokenization process.
9. Integrate masking and tokenization into Continuous Integration/Continuous Delivery (CI/CD) pipelines for DevSecOps.
10. Align data protection techniques with key global regulations: GDPR, HIPAA, CCPA, and PCI DSS.
11. Implement real-time Dynamic Masking for Production Environments based on user roles and access policies.
12. Explore advanced applications in Big Data environments and Cloud Platforms
13. Develop a comprehensive Data Privacy Framework that mitigates insider threats and external breach risks.

Target Audience

1. Data Security Analysts/Engineers
2. Data Architects and Database Administrators (DBAs)
3. DevOps and DevSecOps Engineers
4. Compliance and Risk Officers (GDPR/HIPAA/PCI)
5. Software Developers and QA/Testing Professionals
6. Cloud Engineers managing sensitive data migration
7. Data Scientists and Business Intelligence (BI) Analysts requiring de-identified data
8. IT/Security Managers and C-Suite executives overseeing data strategy

Course Modules

Module 1: Foundational Data Privacy and Risk

- The Data Privacy Landscape.
- Understanding the Data Lifecycle and points of vulnerability
- Case Study: A major financial institution's compliance failure due to unmasked test data exposure.
- Introduction to Data De-Identification.
- Legal and Regulatory Drivers.

Module 2: Static Data Masking (SDM) in Non-Production

- SDM Architecture and Implementation for Test/Dev environments.
- Core SDM Techniques.
- Case Study: Securely provisioning a new offshore QA environment using SDM to protect customer records.
- Ensuring Referential Integrity across linked tables and schemas.
- Designing and applying a complex masking template to a mock relational database.

Module 3: Dynamic Data Masking (DDM) in Production

- Real-time, On-the-Fly masking without altering the source data.
- DDM Architecture.
- Case Study: Implementing DDM for a live Call Center application to ensure agents only see the last four digits of a credit card number.
- Role-Based Access Control and policy configuration for DDM.
- Selecting the right solution for performance and security.

Module 4: Advanced Masking Techniques

- Format-Preserving Encryption.
- Data Redaction and Nulling/Deletion for maximum security.
- Case Study: Migrating a legacy system to the Cloud using FPE to ensure test data is realistic and application-compatible.
- Handling unstructured data masking.
- Masking in Big Data and NoSQL environments.

Module 5: Principles of Data Tokenization

- Tokenization Architecture.
- The Tokenization Process.
- Case Study: Achieving PCI DSS scope reduction by tokenizing all payment card data within an e-commerce platform.
- Reversibility and De-Tokenization controls for authorized processes.
- Difference between Tokenization and Cryptographic Hashing.

Module 6: Tokenization Implementation and Best Practices

- Selecting the right token format
- Securing the Token Vault.
- Case Study: Integrating a tokenization service with an ERP system to protect vendor PII without breaking business logic.
- Tokenization for different data types.
- Monitoring and auditing token usage for compliance reporting.

Module 7: Integration and DevSecOps

- Integrating data de-identification into the CI/CD Pipeline.
- Automated Sensitive Data Discovery and Classification.
- Case Study: Accelerating software releases by automating the creation of compliant test data on-demand.
- Implementing Data Governance policies over masked and tokenized data.
- Best practices for Cloud Data Security Posture Management.

Module 8: Strategy, Tools, and The Future

- Evaluating leading commercial and open-source masking and tokenization tools.
- Developing a business-driven data protection strategy and roadmap.
- Case Study: Designing a hybrid cloud data protection strategy utilizing both dynamic masking for live access and static masking for cloud data migration.
- The future of data protection.
- Developing a comprehensive Data Protection Proposal for a target industry.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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