Data Protection in Digital Financial Services Training Course

Professional Development Training Course Outline

Category	Microfinance & Financial Inclusion	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Access to clean cooking solutions is essential for improving health outcomes, reducing environmental pollution, and promoting social inclusion among low-income populations. Traditional cooking methods relying on firewood or charcoal contribute to respiratory illnesses and environmental degradation, while clean cooking technologies such as LPG stoves, biogas, and improved cookstoves offer sustainable alternatives. Microfinance institutions (MFIs) play a critical role in enabling households to adopt these solutions through affordable, flexible financing options. By integrating clean cooking finance into their portfolios, MFIs support community health, environmental sustainability, and long-term financial inclusion. Microfinance for Clean Cooking Solutions Training Course equips participants with the knowledge and tools to design, implement, and manage effective clean cooking microfinance programs.

Participants will learn practical strategies for assessing demand, structuring loans, and managing portfolios for clean cooking solutions. The course emphasizes digital innovations, partnership development with NGOs, government programs, and energy providers, and risk mitigation strategies to ensure program success. Learners will explore monitoring and evaluation techniques to measure social impact and operational performance. Through case studies and hands-on exercises, participants will gain skills to design scalable, sustainable, and socially impactful clean cooking finance programs. By the end of the course, participants will be able to deliver innovative clean cooking microfinance solutions in diverse contexts.

Programme Curriculum

Data Protection in Digital Financial Services Training Course

Introduction

Data protection has become a core pillar of trust, security, and regulatory compliance in the digital financial services ecosystem. As financial institutions increasingly rely on digital channels, the volume of sensitive customer data collected, processed, and stored continues to grow. This shift has increased the need for robust data protection frameworks, cybersecurity governance, and responsible data management practices. Data Protection in Digital Financial Services Training Course equips participants with the skills needed to safeguard personal data, strengthen privacy controls, and implement global best practices in digital financial services.

The course integrates technical, regulatory, and strategic leadership perspectives, enabling participants to address modern challenges in data security, digital identity, fraud prevention, and risk governance. Participants will explore emerging technologies, international data privacy standards, and practical tools for managing data protection risks. By the end of the course, participants will be able to build secure data environments, ensure compliance across digital platforms, and drive consumer confidence in digital financial systems.

Course Objectives

1. Understand the fundamentals of data protection in digital financial services.
2. Apply global data privacy standards within financial ecosystems.
3. Strengthen cybersecurity governance and risk management practices.
4. Implement secure data collection, processing, and storage systems.
5. Identify and mitigate emerging threats in digital financial platforms.
6. Conduct data protection impact assessments.
7. Enhance digital identity management and authentication mechanisms.
8. Promote responsible data usage and ethical handling practices.
9. Improve fraud detection and response frameworks.
10. Strengthen incident response and disaster recovery planning.
11. Ensure regulatory compliance in data protection.
12. Integrate data protection into digital transformation initiatives.
13. Monitor and evaluate data protection controls.

Organizational Benefits

- Enhanced consumer trust and institutional reputation
- Strengthened cybersecurity posture and reduced vulnerabilities
- Improved compliance with national and international regulations
- Reduced risks of data breaches and financial losses
- Increased operational efficiency in data management
- Better fraud prevention and detection capabilities
- Improved data governance frameworks
- Stronger digital service delivery channels
- Better preparedness for audits and regulatory inspections
- Reduced legal liabilities and privacy-related penalties

Target Audiences

1. Financial regulators
2. Digital financial service providers
3. Bank and fintech data managers
4. Cybersecurity officers
5. Compliance and audit professionals
6. Microfinance leaders

7. ICT and digital transformation staff
8. Risk management specialists

Course Duration: 10 days

Course Modules

Module 1: Introduction to Data Protection in Digital Finance

- Key concepts and definitions
- Importance of data protection in financial services
- Overview of digital financial ecosystems
- Data risk categories in digital platforms
- Case study: Data breach impacts on financial institutions
- Class activity: Identifying sensitive data types

Module 2: Global Data Privacy Standards and Regulations

- GDPR, ISO standards, and emerging regulations
- Regional regulatory frameworks
- Compliance requirements for DFS providers
- Cross-border data flow considerations
- Case study: Regulatory enforcement actions
- Group task: Mapping regulatory obligations

Module 3: Data Governance in Digital Financial Services

- Principles of data governance
- Data ownership and stewardship models
- Data quality and lifecycle management
- Organizational roles and responsibilities
- Case study: Building a data governance framework
- Practical exercise: Drafting a governance structure

Module 4: Cybersecurity Principles for DFS

- Cybersecurity fundamentals
- Threat landscapes in digital finance
- Security controls and best practices
- Securing digital platforms and apps
- Case study: Cyberattack on a mobile money provider
- Hands-on activity: Threat identification

Module 5: Digital Identity Management and Authentication

- Digital identity systems
- Biometrics and multi-factor authentication
- Risks associated with weak identification systems
- Digital KYC requirements
- Case study: Implementing secure digital identity
- Exercise: Evaluating an ID management system

Module 6: Data Collection, Processing, and Storage Controls

- Secure data collection methods
- Encryption and anonymization techniques
- Data minimization principles
- Cloud storage and local storage considerations
- Case study: Securing customer databases
- Lab: Designing secure data flows

Module 7: Fintech Security and Technology Risks

- Vulnerabilities in fintech systems
- API security and integration risks
- Mobile app and USSD protection
- Vendor risk management
- Case study: Fintech security failure analysis
- Simulation: Identifying fintech risks

Module 8: Fraud Prevention and Detection in DFS

- Types of financial fraud
- Digital fraud detection tools
- AI and machine-learning-based fraud systems
- Customer protection strategies
- Case study: Fraud detection success story
- Group exercise: Fraud response planning

Module 9: Data Protection Impact Assessments (DPIA)

- DPIA frameworks and methodologies
- Identifying data risks in new products
- Assessing technological and operational risks
- Documentation and reporting requirements
- Case study: DPIA for a new mobile app
- Workshop: Conducting a mini-DPIA

Module 10: Ethical Data Use and Consumer Protection

- Principles of ethical data handling
- Informed consent and transparency
- Preventing exploitation through data misuse
- Consumer rights in digital platforms
- Case study: Ethical dilemmas in DFS
- Discussion: Creating ethical guidelines

Module 11: Incident Response and Crisis Management

- Incident response planning
- Detecting and reporting data breaches
- Crisis communication strategies
- Coordination with regulators and stakeholders
- Case study: Major DFS data breach response

- Exercise: Developing an incident response plan

Module 12: Business Continuity and Disaster Recovery Planning

- Business continuity frameworks
- Backup and restoration strategies
- Disaster recovery for digital systems
- Testing continuity plans
- Case study: Disaster recovery after cyberattack
- Simulation: Drafting a recovery plan

Module 13: Data Monitoring and Evaluation Tools

- Data monitoring indicators
- Evaluating data security controls
- Audit trails and accountability systems
- Continuous improvement mechanisms
- Case study: Monitoring failures and lessons
- Practical activity: Designing M&E indicators

Module 14: Integrating Data Protection in Digital Transformation

- Role of data security in digital innovation
- Organizational change management
- Aligning digital products with security needs
- Staff capacity-building strategies
- Case study: Digital transformation with strong privacy controls
- Exercise: Creating integration plans

Module 15: Emerging Technologies and Future Trends

- AI, IoT, and blockchain privacy considerations
- Future regulatory expectations
- Data protection challenges in evolving DFS systems
- Innovation vs. security balance
- Case study: AI-driven data protection model
- Workshop: Predicting future data risks

Training Methodology

- Interactive instructor-led presentations
- Case study analysis and group discussion
- Practical exercises and simulations
- Hands-on system evaluation and risk assessments
- Role-play for incident management
- Workshops on regulatory compliance and governance frameworks

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