Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

MONITORING AND EVALUATION

Data Security and Confidentiality in M&E Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
10 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 21, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE
P.O. Box 102802-00101, Nairobi, Kenya
Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy
Tel: +254 724 527 104 | +254 734 969 612
Email: training@datastatresearch.org
www.datastatresearch.org

Data Security and Confidentiality in M&E Training Course

Monitoring and Evaluation • 10 Days Intensive • Accredited Certification

Course Overview

Data Security and Confidentiality in M&E Training Course equips M&E professionals with practical strategies, tools, and frameworks to safeguard sensitive data while ensuring high-quality data collection, storage, analysis, and reporting.

Key Skills & Software Tools Covered

Access control • data encryption • privacy compliance • secure storage

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
12 Jan 2026 – 23 Jan 2026	Nairobi	Classroom / 10d	**$3,000 USD / KES 220,000**
12 Jan 2026 – 23 Jan 2026	Kigali	Classroom / 10d	**$6,000 USD / KES 110,000**
12 Jan 2026 – 23 Jan 2026	Dubai	Classroom / 10d	**$10,000 USD / KES 110,000**
12 Jan 2026 – 23 Jan 2026	Cape Town	Classroom / 10d	**$9,000 USD / KES 110,000**
12 Jan 2026 – 23 Jan 2026	Addis Ababa	Classroom / 10d	**$6,000 USD / KES 110,000**
12 Jan 2026 – 23 Jan 2026	Singapore	Classroom / 10d	**$10,000 USD / KES 110,000**
12 Jan 2026 – 23 Jan 2026	Istanbul	Classroom / 10d	**$10,000 USD / KES 110,000**
12 Jan 2026 – 23 Jan 2026	Bangkok	Classroom / 10d	**$10,000 USD / KES 110,000**
12 Jan 2026 – 23 Jan 2026	Accra	Classroom / 10d	**$8,000 USD / KES 110,000**
26 Jan 2026 – 6 Feb 2026	Nairobi	Classroom / 10d	**$3,000 USD / KES 220,000**
26 Jan 2026 – 6 Feb 2026	Kigali	Classroom / 10d	**$6,000 USD / KES 110,000**
26 Jan 2026 – 6 Feb 2026	Dubai	Classroom / 10d	**$10,000 USD / KES 110,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

Data Security and Confidentiality in M&E Training Course

Introduction

In the digital era, data security and confidentiality are critical pillars for effective Monitoring and Evaluation (M&E). Organizations face increasing challenges from data breaches, unauthorized access, and privacy violations, which can compromise program integrity, stakeholder trust, and compliance with data protection regulations. Data Security and Confidentiality in M&E Training Course equips M&E professionals with practical strategies, tools, and frameworks to safeguard sensitive data while ensuring high-quality data collection, storage, analysis, and reporting. Participants will gain a deep understanding of data governance, cybersecurity best practices, ethical data handling, and legal compliance to enhance accountability and program impact.

This course emphasizes the integration of cutting-edge security technologies, encryption protocols, risk assessment techniques, and privacy-by-design approaches in M&E systems. Using real-world case studies, hands-on exercises, and interactive discussions, learners will develop the skills to implement robust data protection policies, mitigate risks of data leaks, and manage access control across various digital platforms. By the end of this training, participants will be confident in protecting sensitive information, maintaining stakeholder trust, and aligning M&E practices with global data security standards.

Course Duration

10 days

Course Objectives

- Understand core principles of data security and confidentiality in M&E.
- Apply data protection frameworks and regulatory compliance standards.
- Identify potential data threats and vulnerabilities in M&E systems.
- Implement effective access control and user authentication strategies.
- Master encryption techniques and secure data storage solutions.
- Ensure ethical handling of personal and sensitive data.
- Conduct data risk assessments and mitigation planning.
- Establish privacy-by-design processes for M&E data collection.
- Develop incident response and breach management protocols.
- Apply secure data sharing and collaboration practices.
- Integrate cybersecurity best practices into M&E workflows.
- Analyze real-world case studies of data breaches and lessons learned.
- Foster a culture of data security awareness among M&E teams.

Target Audience

- M&E Officers and Specialists
- Program Managers
- Data Analysts and Researchers
- IT and Cybersecurity Professionals supporting M&E
- NGO and Development Organization Staff
- Policy Makers and Compliance Officers
- Field Data Collection Teams
- Anyone responsible for data management and reporting in programs

Course Modules

Module 1: Introduction to Data Security in M&E

- Importance of data security in program evaluation
- Key concepts: confidentiality, integrity, availability
- Overview of global data protection regulations
- Data lifecycle in M&E systems
- Case Study: Unauthorized data access in a healthcare survey

Module 2: Legal and Ethical Frameworks

- GDPR, HIPAA, and local data protection laws
- Ethical principles in data handling
- Consent and anonymization of data
- Compliance audits and reporting
- Case Study: Breach of participant confidentiality in a nutrition program

Module 3: Data Governance and Policies

- Designing a data governance framework
- Roles and responsibilities of data stewards
- Policy development and enforcement
- Monitoring compliance within teams
- Case Study: NGO’s implementation of a data governance policy

Module 4: Risk Assessment and Threat Modeling

- Identifying internal and external threats
- Vulnerability analysis for M&E systems
- Risk scoring and prioritization
- Developing mitigation strategies

- Case Study: Risk assessment of mobile survey tools

Module 5: Data Access Control

- Role-based access and user permissions
- Authentication and multi-factor security
- Managing third-party access
- Audit trails and monitoring
- Case Study: Misuse of field data access in a community survey

Module 6: Encryption and Secure Storage

- Principles of data encryption at rest and in transit
- Securing cloud storage and local databases
- Backup and disaster recovery planning
- File-level and database encryption techniques
- Case Study: Encrypted survey data protection in emergency settings

Module 7: Secure Data Collection

- Mobile and online survey security
- Protecting data during field collection
- Ensuring secure offline storage
- Data validation without compromising confidentiality
- Case Study: Field survey data breach due to insecure devices

Module 8: Data Sharing and Collaboration

- Secure file sharing platforms
- Data sharing agreements and MOUs
- Redaction and anonymization techniques
- Collaboration tools with built-in security features
- Case Study: Cross-organization data sharing gone wrong

Module 9: Incident Management

- Detecting and reporting data breaches
- Incident response protocols
- Forensic analysis of breaches
- Post-incident review and learning
- Case Study: Response to a M&E dataset leak in a donor-funded program

Module 10: Privacy by Design in M&E Systems

- Embedding privacy into system architecture
- Minimizing personal data collection
- Pseudonymization and anonymization strategies
- Monitoring compliance with privacy principles
- Case Study: Designing a privacy-first health survey

Module 11: Cybersecurity Best Practices

- Password hygiene and credential management
- Antivirus, firewalls, and security updates
- Safe use of emails and communication platforms
- Network monitoring and intrusion detection
- Case Study: Preventing ransomware attacks on M&E servers

Module 12: Cloud Security for M&E

- Cloud storage risk assessment
- Securing cloud-based analytics platforms
- Identity and access management in the cloud

- Compliance with cloud security standards
- Case Study: Cloud data compromise in an education program

Module 13: Data Quality and Integrity

- Ensuring accuracy without compromising security
- Audit trails and version control
- Secure data cleaning and validation
- Preventing unauthorized modifications
- Case Study: Manipulated survey results in a field study

Module 14: Training and Capacity Building

- Building a culture of data security
- Staff training modules and exercises
- Simulated breach scenarios
- Continuous professional development
- Case Study: Improving M&E team security awareness in an NGO

Module 15: Emerging Trends in Data Security

- AI and blockchain for data protection
- IoT and sensor data security
- Predictive analytics for threat detection
- Future-proofing M&E systems
- Case Study: Use of AI to detect anomalies in health survey data

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@datastatresearch.org or call +254724527104

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 DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/data-security-and-confidentiality-in-m-e-training-course to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.