AI & DIGITAL · SHORT COURSE

Responsible AI and Cybersecurity Awareness for Public Institutions

This practical course equips public-sector managers, ICT professionals, administrators, policymakers, and employees with the knowledge and practical skills required to understand, adopt, and use Artificial Intelligence (AI) responsibly while strengthening cybersecurity awareness within public institutions.

DATES	14–18 Dec 2026	DURATION	5-day course
COURSE FEE	TZS 1,200,000 · per participant	VAT	Fee excludes VAT
VENUE	Arusha, Tanzania	DAILY HOURS	8:30 AM – 4:30 PM
FEE INCLUDES	Course materials, lunch and refreshments	CERTIFICATE	Certificate of attendance
TRAINER	Elly International training team	APPLICATIONS	Open for applications

Overview

This practical course equips public-sector managers, ICT professionals, administrators, policymakers, and employees with the knowledge and practical skills required to understand, adopt, and use Artificial Intelligence (AI) responsibly while strengthening cybersecurity awareness within public institutions.

Participants will explore the opportunities and risks associated with Generative AI, including AI-assisted productivity, information analysis, document preparation, communication, decision support, and public service delivery. The course emphasizes responsible AI principles such as transparency, accountability, privacy, fairness, human oversight, information accuracy, and ethical use.

The cybersecurity component focuses on strengthening organizational awareness and reducing human-related security risks. Participants will learn how to identify common cyber threats, protect institutional information, recognize phishing and social engineering attacks, manage passwords and access securely, protect devices and data, and respond appropriately to cybersecurity incidents.

Through practical demonstrations, case studies, simulations, group exercises, and workplace-based scenarios, participants will develop practical approaches for responsible AI adoption and stronger cybersecurity awareness while supporting institutional governance, public trust, confidentiality, and service continuity.

Course content

Module 1: Introduction to Artificial Intelligence in Public Institutions

- Introduction to Artificial Intelligence and Generative AI
- Understanding Large Language Models and AI assistants
- Applications of AI in public-sector environments
- AI for productivity and administrative tasks
- AI for research, analysis and decision support
- Opportunities and benefits of AI in public service delivery
- Limitations and risks of AI systems

- Human judgment and oversight in AI-supported activities
- AI adoption challenges in public institutions

Module 2: Responsible AI Principles and Governance

- Meaning and principles of responsible AI
- Transparency and explainability
- Accountability and responsibility
- Fairness and non-discrimination
- Human oversight and meaningful human control
- Accuracy, reliability and verification
- Managing AI bias and potential discrimination
- Ethical use of AI in public administration
- AI governance frameworks and institutional policies
- Developing responsible AI practices within public institutions

Module 3: Data Privacy, Confidentiality and AI Security

- Understanding personal and sensitive information
- Data privacy and confidentiality principles
- Risks of entering institutional information into public AI tools
- Protection of government and institutional data
- Data classification and handling
- Secure use of AI applications
- Privacy risks associated with AI-generated content
- Data leakage and information exposure
- Third-party AI services and security considerations
- Practical guidelines for secure AI use

Module 4: Cybersecurity Fundamentals for Public Institutions

- Introduction to cybersecurity
- Cybersecurity principles and the CIA Triad
- Common cyber threats facing public institutions
- Malware, ransomware and spyware
- Phishing and spear-phishing
- Social engineering attacks
- Business email compromise
- Credential theft and account compromise
- Insider threats
- Website and application security risks
- Cybersecurity risks associated with remote and mobile working

Module 5: Identity, Access and Password Security

- Importance of identity and access management
- Strong password practices
- Password managers and secure credential storage
- Multi-factor authentication (MFA)
- Account protection and access control
- Principle of least privilege
- User account security
- Privileged account awareness
- Secure handling of authentication information

- Recognizing compromised accounts
- Practical password and authentication exercises

Module 6: Phishing, Social Engineering and Human-Centred Security

- Understanding social engineering
- Phishing email identification
- Smishing and vishing attacks
- Impersonation and fraudulent requests
- Social media-based attacks
- Psychological techniques used by attackers
- Identifying suspicious links and attachments
- Verifying unusual requests
- Reporting suspected phishing and fraud
- Practical phishing awareness simulations
- Building a security-conscious organizational culture

Module 7: Secure Devices, Networks and Information

- Secure use of computers and mobile devices
- Operating system and software updates
- Antivirus and endpoint protection
- Secure use of removable storage devices
- Safe use of public and institutional Wi-Fi
- Secure remote access and VPN awareness
- Encryption and secure file sharing
- Backup and recovery principles
- Protection against ransomware
- Physical security of ICT equipment
- Secure disposal of institutional information and devices

Module 8: AI-Related Cybersecurity Risks

- Cybersecurity risks associated with Generative AI
- AI-generated phishing and social engineering
- Deepfakes and synthetic media
- AI-assisted fraud and impersonation
- Malicious use of AI by cybercriminals
- Prompt injection and AI application security risks
- Sensitive information exposure through AI tools
- AI-generated misinformation and manipulation
- Verifying AI-generated information
- Protecting institutional AI systems and data
- Human oversight and security controls

Module 9: Cybersecurity Incident Awareness and Response

- Understanding cybersecurity incidents
- Recognizing signs of compromise
- Incident reporting procedures
- Immediate actions following a suspected cyber incident
- Phishing and malware response
- Lost or stolen device response
- Account compromise response

- Data breach awareness
- Incident escalation and communication
- Business continuity and service resilience
- Lessons learned and post-incident improvement

Module 10: AI, Digital Ethics and Public Trust

- AI and public-sector ethics
- Responsible use of AI-generated information
- Preventing misinformation and disinformation
- Verification and fact-checking
- Bias and fairness in automated decision-making
- Transparency in AI-supported public services
- Protecting citizens' information
- Accountability for AI-assisted decisions
- Maintaining public trust in digital services
- Balancing innovation, security and responsible governance

Module 11: Practical Responsible AI and Cybersecurity Awareness Programme

- Developing an institutional responsible AI framework
- Developing an AI acceptable-use guideline
- Conducting a basic cybersecurity awareness assessment
- Identifying common institutional cyber risks
- Developing an employee cybersecurity checklist
- Phishing identification and response exercise
- Secure AI use case development
- Data protection and AI risk assessment exercise
- Developing an incident reporting workflow
- Creating an institutional AI and cybersecurity awareness action plan
- Group case studies and practical presentations

Who should attend

This course is designed for:

- Public-sector managers and executives
- Government administrators and officers
- ICT and information security professionals
- Human resource officers
- Records and information management officers
- Data protection and privacy officers
- Policy and planning officers
- Public relations and communication officers
- Finance and procurement officers
- Monitoring and evaluation professionals
- Internal auditors and compliance officers
- Programme and project managers
- Customer and public service officers
- Administrative and support staff
- Employees responsible for handling institutional information
- Senior officials responsible for digital transformation and governance

Suitable Sectors

The course is particularly relevant to government ministries, departments and agencies, local government authorities, public institutions, regulatory authorities, parastatals, universities and educational institutions, public hospitals and healthcare institutions, courts and justice institutions, development organizations, and other public-sector organizations responsible for managing institutional information, digital services, and citizen data.

How to apply

Apply online at ellyinternational.co.tz. Your place is confirmed only after we review your application and contact you, within 1 working day.

Apply for this course | **Ask on WhatsApp** | **Email us**

+255 757 066 880 · training@ellyinternational.co.tz · Boma Road, Arusha, Tanzania · P.O. Box 13424

Details correct as of 28 November 2026.