



KPY-POPS-007

# INTERNAL TRAINING POLICY

## PROCESS OBJECTIVE (PURPOSE)

- To ensure that all Koraites are effectively trained and adopt the right culture towards training within the entire company.

## REQUIREMENTS

- There will be a time and date deadline for each training.
- “Failure” will be defined as the inability or unwillingness to complete a training course as required by the facilitator.
- “Complete Training Course” means completing all aspects of a training session, including training material, training surveys/evaluations, and knowledge tests.
- Kora maintains an enterprise pass mark of 80% for all training; **failure to pass some tests may be reported as incomplete training.**
- Compliance and Information Security training and awareness go hand in hand.
- “Training Units” are the units of the organisation approved to provide training and education to employees. This includes the following:
  1. Compliance and Risk Management Unit.
  2. Information Security Unit.
  3. Any other unit approved by the People & Culture team to provide training

## PROCESS FLOW

- The training units each have training scheduled per month. See the training calendar [here](#).
- All training notifications will roll out within the first three business days at the beginning of the month.
- After this is done, there is a mandatory period to complete the training(s). Training must be completed no later than the day before the last day of the month
- Within the mandatory period, the training units may send out reminders (maximum of 4 times).
- By the end of the training period, the training unit must send a notification email to the Line Manager of all employees with outstanding training, asking them to schedule a meeting with the employee and document this.
- By the next month, an email from the People & Culture team will be sent to all employee(s) with outstanding training for a meeting with the People & Culture Manager, and a **warning letter** will be sent with the CEO and COO in copy.
- Employees can only have one warning letter on their file, after which a **final warning letter** will be issued.
- **Employees can only have one final warning letter per calendar year; further infractions will result in a one-month suspension without pay up to termination of employment.**
- There will be Phishing remedial training every month for those who fail phishing tests
- Training reminders sent to all employees will include penalties for failing to complete training within the stipulated time
- Team leads will receive email notifications of team members with outstanding training, and training default penalties 3 days before the training deadline.
- Infosec & Compliance training, and phishing test performance would be included in employee OKRs and departmental OKRs.

- Monthly reports would include statistics (names, departments) of those who fail to complete training and/or fail phishing tests
- Monthly newsletters from the People Ops team would include statistics (departments) of those who fail to complete training and/or fail phishing tests

Refer to the [Disciplinary and Grievance policy](#).

#### COMPLIANCE & RISK MGT TRAINING PLAN

S/N	Course	Duration (Hours)	Trainers	Participants	Month
1	Ethics, Code of Conduct	1	Enyioma Madubuike	All staff and directors	January
2	Anti-Financial Crimes: Payments Fraud, Transaction and Cyber Laundering	1	Enyioma Madubuike	All staff and directors	February
3	Conflicts of Interest	1	Enyioma Madubuike	All staff and directors	March
4	Business Continuity management systems	1	Enyioma Madubuike	All staff and directors	April
5	Confidential Information and Privacy of Communication	1	Enyioma Madubuike	All staff and directors	May
6	Anti-money Laundering and Combating Financing of Terrorism	1	Enyioma Madubuike	All staff and directors	June
7	Company Assets and Transactions	1	Enyioma Madubuike	All staff and directors	July
8	Anti-Bribery and Corruption	1	Enyioma Madubuike	All staff and directors	August
9	Anti-Financial Crimes: Money laundering	1	Enyioma Madubuike	All staff and directors	September

10	Data Security, protection, and Privacy	1	Enyioma Madubuike	All staff and directors	October
11	Suspicious transactions & activities escalation and reporting	1	Enyioma Madubuike	All staff and directors	November
12	Business Continuity Management System	1	Enyioma Madubuike	All staff and directors	December

## INFORMATION SECURITY TRAINING AND AWARENESS PLAN

Course Outline	Applicable Standard	Name of Trainer	Recipient	Schedule	Platform
Cyber Hygiene Essentials - Phishing Emails: Think Before You Act - Cyber Essentials - Sharing Safely on Social Media - Cyber Essentials Series: Working Remotely - Safe Web Browsing	PCI DSS ISO 27001 FFIEC	Antonella Akosa	All staff	January	Knowbe4
Artificial Intelligence - World Wild Web: Using AI Tools For Work - AI, Phishing, and Cybersafety - Generative AI: Seeing Through the Deception - AI and Sensitive Info Don't Mix	ISO 27032 ISO 27017	Antonella Akosa	All staff	February	Knowbe4
Payment Card Security - PCI DSS 4.0: Getting To Know the Payment Card Industry Data Security Standard - How To Handle Payment Card Data	PCI DSS	Antonella Akosa	All staff	March	Knowbe4
Emerging Cyber Threats - Kickoff: Overview Cyberattacks - Ransomware: Blackmail Using Encrypted Data - QR Code Phishing - Malware - USB Attacks: Small Devices, Big Threats	PCI DSS ISO 27001 FFIEC ISO 27032 ISO 27017	Antonella Akosa	All staff	April	Knowbe4

- Confessions of a video caller					
Data Classification & Protection - Data protection - How it works - Data Protection with Quiz - Cyber Essentials Series: Information Classification 101 - Data Classification and Handling - Your role as a privileged user	NDPA GDPR	Antonella Akosa	All staff	May	Knowbe4
Artificial Intelligence - AI At Work: Use It Wisely - AI Scams: New Dangers - AI: New Tools and New Threats - Generative AI: Intelligent and Dangerous?	ISO 22301	Antonella Akosa	All staff	June	Knowbe4
Cloud Security - Cloud Services - Secure Cloud Administration - Criminal Minds: Cloud Apps	ISO 27017	Antonella Akosa	All staff	July	Knowbe4
Mobile and Remote Work Security - Mobile Device Security - Home Sweet Home Office - Secure Remote Work - Remote Work: Physical Security	PCI DSS ISO 27001 FFIEC ISO 27032	Antonella Akosa	All staff	August	Knowbe4
Data Privacy - Data Privacy Basics - The What, Why & How of Data Privacy - Privacy Series: Personal Information at Work - Privacy Series: Prevent Identity Theft	NDPA GDPR	Antonella Akosa	All staff	September	Knowbe4
Incident Reporting - Reporting Security Incidents - How To Use the Phish Alert Button for Gmail - Make it a Habit ... PAB it! - Security Bytes: Incident Reporting - See Something, Say Something - Perspectives with Quiz: Incident Reporting	PCI DSS ISO 27001 FFIEC ISO 27032 ISO 27017 ISO 22301	Antonella Akosa	All staff	October	Knowbe4
Password Management & Authentication - Cybersecurity Essentials: Secure Passwords - A Guide to Avoiding Password Reuse - Protect What Is Valuable - Confessions of a Password Recycler		Antonella Akosa	All staff	November	Knowbe4

- Security Bytes: Multi-Factor Authentication					
Third Party Security - Working With Third Parties Securely - Navigating the Shadows: Supply Chain Security		Antonella Akosa	All staff	December	Knowbe4

INFORMATION SECURITY TRAINING & AWARENESS PLAN (SPECIFIC GROUPS) - 2025					
Course Outline	Applicable Standard	Name of Trainer	Recipient	Schedule	Platform
- Leadership Series: Phishing the Executive - Security for Sales	PCI DSS ISO 27001 FFIEC NDPA ISO 22301	Antonella Akosa	Team Leads Sales	January	Knowbe4
- Secure Coding 04: OWASP Top 10 - Your Role as a Privileged User		Antonella Akosa	Engineering InfoSec	February	Knowbe4
- Security for Human Resources - Finance Sector Phishing with Quiz		Antonella Akosa	People Ops Finance	April	Knowbe4
- Reality Bytes: Vishing - GDPR For Marketing - Privacy and Security		Antonella Akosa	Merchant Success Marketing Legal	May	Knowbe4
A Request from the Top? CEO Fraud		Antonella Akosa	Team Leads	June	Knowbe4
- Supply Chain Attacks - Supply Chain Cyber Security		Antonella Akosa	Product Design Product Development Operations	August	Knowbe4
- Secure Application Development: Protecting Source Code - Security Culture: Compliance		Antonella Akosa	Engineering Compliance	September	Knowbe4
- Secure Hiring and Onboarding - Securing Client Personal Data in the Workplace		Antonella Akosa	People Ops Data	October	Knowbe4
- Reporting Privacy Incidents - Crisis Management		Antonella Akosa	Incident Response	November	Knowbe4