MALLAH

Data Protection & Information Security

Training & Awareness Program

How Mallah Company prepares its people to protect information

MALLAH COMPANY

ISSUED BY	Mallah Company (Lemallah) A family-owned group of businesses operating in Syria since 1970 · Offices in Aleppo and Damascus
DOCUMENT NO.	MC-POL-004 · Version 1.0
OWNER / REVIEW	Legal Department Manager · Reviewed at least annually
APPROVED BY	Mohamed Almallah, Managing Director
CLASSIFICATION	Shareable with clients and business partners

Document Control

Title	Data Protection & Information Security Training & Awareness Program
Issued by	Mallah Company (Lemallah)
Document no. / version	MC-POL-004 · v1.0
Owner	Legal Department Manager
Applies to	All employees, managers, office, booking and dispatch staff, IT, finance and HR personnel, drivers and site staff where relevant, contractors and consultants with access to information of Mallah Company or any group company
Approved / next review	September 2026 / September 2027 (reviewed at least annually)
Classification	Shareable with clients and business partners
Basis	Builds on the confidentiality rules already applied in the group companies, including TaxiTel's Data Protection Training Program (TT-POL-004); supports MC-POL-002 and MC-POL-003

Contents

1 Purpose 3
2 Scope 3
3 Training Requirements 3
4 Core Training Topics 4
5 Delivery Methods 5
6 Awareness Activities 5
7 Training Records 5
8 Measuring Effectiveness 6
9 Roles and Responsibilities 6
10 Non-Compliance 6
11 Program Review and Approval 6

SECTION 01

1 Purpose

Mallah Company is committed to protecting personal, client, employee, operational, financial and business information against unauthorised access, disclosure, alteration, loss or misuse. People are the first line of that protection.

This Program makes sure that employees and other authorised users across all group companies understand their responsibilities when handling company information and using company systems. It supports the group's Privacy Policy (MC-POL-002) and Records Management and Data Retention Policy (MC-POL-003).

SECTION 02

2 Scope

This Program applies to everyone given access to information or information systems of Mallah Company or any group company — TaxiTel, Node Trade, Node Construction, Node Multiservice, Monoland, Mallah for Travel and Adams Jeans — including:

- management and office staff;
- booking, sales, call-centre and dispatch personnel;
- finance, administration and human resources personnel;
- IT personnel;
- drivers, site and venue staff, for the parts relevant to their work; and
- contractors and consultants.

Training content is adjusted to each person's role and level of access.

SECTION 03

3 Training Requirements

3.1 Induction training

Employees who will have access to company systems, customer information, employee information, financial information or confidential business information receive basic data-protection and information-security training as part of their induction — where practical, before or shortly after their system access is granted.

3.2 Annual refresher training

Relevant employees receive refresher training at least once a year. Additional training is provided when significant new systems are introduced, security procedures change, an incident reveals a training need, new client or contractual requirements apply, or management identifies a specific risk.

3.3 Role-specific training

Employees with higher levels of access or responsibility receive additional training suited to their role — in particular those working in IT and system administration, finance, human resources, booking and dispatch, contract administration and management, and anyone handling sensitive client, customer or traveller information.

3.4 Drivers, site and venue staff

Drivers, site and venue staff receive practical, scenario-based briefings in Arabic on protecting customer and visitor privacy: keeping customer details confidential, not photographing or posting about customers or visitors — especially children — protecting phones that contain customer details, and reporting a lost device immediately.

SECTION 04

4 Core Training Topics

TOPIC	WHAT EMPLOYEES LEARN
Confidentiality	Why company and client information must be protected; access only for legitimate business purposes; no disclosure without authorisation; proper handling of information about clients, customers, employees, suppliers and operations.
Personal and customer information	Collect only what is needed; avoid unnecessary sharing; confirm recipients before sending sensitive information; prevent others from viewing customer, client or employee data; report accidental disclosure or loss promptly.
Password security	Use strong passwords; keep them secret and never share them; do not reuse company passwords for personal services; lock devices when unattended; report suspected compromise immediately; use multi-factor authentication where the company requires it.
Phishing and suspicious messages	Recognise requests for passwords, suspicious links or attachments, unusual payment instructions, false urgency, requests to change bank details, and impersonation of managers, clients or suppliers; verify unusual requests through a separate channel; report them.
Payment and supplier fraud	Be alert to fake invoices and changed bank details from suppliers — including foreign suppliers — and confirm any change by phone using known contact details before paying.
Email and messaging	Check recipients before sending confidential information; use company-approved channels; do not forward company documents to personal accounts without authorisation; take care with messaging applications.
Safe use of devices	Take care with computers, phones, tablets, removable storage and remote access; never disable security controls; report lost or stolen devices immediately.
Physical security	Do not leave confidential documents unattended; store sensitive files securely; prevent others from viewing screens; dispose of sensitive paper securely; report suspicious access.

TOPIC	WHAT EMPLOYEES LEARN
Access control	Access only what your duties require; never use another person's account, bypass access restrictions, or give system access to unauthorised people.
Software and external services	Do not install unauthorised software or download suspicious files; do not upload company information to unauthorised websites, cloud-storage, file-sharing or AI services; follow company instructions on approved tools.
Social engineering	Attackers may pretend to be management, IT support, clients, suppliers, banks, government bodies or colleagues; verify unusual requests before giving information, credentials or access.
Incident reporting	Report promptly — even when unsure — any wrong recipient, lost device or paper records, suspicious login, malware, phishing, stolen credentials, unauthorised access, accidental deletion or disclosure of confidential information.

SECTION 05

5 Delivery Methods

Training and awareness may be delivered through classroom sessions, online meetings, presentations, written guidance, induction, internal notices, security reminders, email awareness messages, practical phishing examples and management briefings. The format is adapted to employees' roles, companies, locations, operational needs and available resources.

SECTION 06

6 Awareness Activities

Formal training is supplemented during the year with awareness activities such as password-security reminders, phishing warnings, data-handling reminders, security notices, lessons learned from incidents, and alerts about emerging threats, so that awareness does not rely only on the annual session.

SECTION 07

7 Training Records

The group keeps records of formal training, including the employee's name, group company, department or role, training date and topic, the trainer or responsible person, and attendance confirmation with the employee's signature or electronic acknowledgement. Training records are kept in line with the Records Management and Data Retention Policy (MC-POL-003) — for the duration of employment plus 5 years.

SECTION 08

8 Measuring Effectiveness

The group may assess whether training is working through short quizzes, verbal checks, simulated phishing exercises, review of security incidents, employee feedback and management review. Repeated incidents or weaknesses lead to additional training for the people or teams concerned.

SECTION 09

9 Roles and Responsibilities

WHO	RESPONSIBILITY
Managing Director	Approves this Program and ensures resources are available to deliver it across the group.
Legal Department Manager	Owns this Program; sets the annual training plan; ensures training records are kept; reviews incidents for training needs.
IT function	Supports the technical content of training, including passwords, phishing, devices and system access, and runs awareness reminders.
Human resources and company managers	Schedule induction and refresher sessions, organise briefings for drivers, site and venue staff, and collect attendance and acknowledgement records.
All employees	Attend required training; follow security procedures; protect company information; ask when unsure; report incidents promptly; cooperate with investigations.

SECTION 10

10 Non-Compliance

Failure to follow information-security and confidentiality requirements may lead to corrective measures or disciplinary action under company procedures. Deliberate misuse or unauthorised disclosure of company information may also lead to contractual or legal action.

SECTION 11

11 Program Review and Approval

This Program is reviewed at least once a year by the Legal Department Manager, and sooner after significant changes in technology, a significant security incident, new client requirements, new information-security risks or material operational changes.

Approval

This Data Protection and Information Security Training & Awareness Program is approved by Mallah Company and applies throughout the group.

NAME _____ TITLE _____

SIGNATURE _____ DATE _____

COMPANY STAMP _____