Records Management & Data Retention Policy

How TaxiTel keeps, protects, archives and disposes of its records

T A X I T E L

ISSUED BY	MHD Nael Almallah & His Partners Co. (TaxiTel) Ground transportation across Syria since 2004 · Offices in Aleppo and Damascus
DOCUMENT NO.	TT-POL-003 · 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	Records Management & Data Retention Policy
Issued by	MHD Nael Almallah & His Partners Co. (TaxiTel)
Document no. / version	TT-POL-003 · v1.0
Owner	Legal Department Manager
Applies to	All employees, managers, drivers, contractors and consultants who create, access or manage TaxiTel records, in electronic or paper form
Approved / next review	September 2026 / September 2027 (reviewed at least annually)
Classification	Shareable with clients and business partners
Basis	Consolidates the record-keeping practices TaxiTel already follows in its operations and its contracts with UN agencies and international NGOs; aligned with TT-POL-001 and TT-POL-002

Contents

1	Purpose	3
2	Scope	3
3	General Principles	4
4	Roles and Responsibilities	4
5	Records Classification	5
6	Data Retention Schedule	5
7	Client and Passenger Information	7
8	Electronic Records and Information Security	8
9	Physical Records	8
10	Backups	8
11	Legal Hold and Suspension of Deletion	8
12	Secure Disposal	9
13	Third Parties and Service Providers	9
14	Loss or Breach of Records	9
15	Employee Departure and Change of Duties	10
16	Monitoring, Exceptions and Non-Compliance	10
17	Policy Review and Approval	10

SECTION 01

1 Purpose

TaxiTel recognises the importance of properly managing, protecting, retaining, archiving and disposing of company information and records. This Policy sets consistent rules for managing business records and data throughout their lifecycle, so that information is:

- retained for legitimate business, contractual, financial, operational and legal purposes;
- protected against unauthorised access, loss, alteration or disclosure;
- available when required for operational, audit, contractual or legal purposes; and
- securely deleted, destroyed or anonymised when it is no longer required.

This Policy puts in writing, in one document, the record-keeping practices TaxiTel already follows in its operations and in its contracts with United Nations agencies, international NGOs and other partners. It works together with TaxiTel's **Privacy Policy (TT-POL-002)** and **Anti-Corruption & Anti-Bribery Policy (TT-POL-001)**.

SECTION 02

2 Scope

This Policy applies to all TaxiTel employees, managers, drivers, contractors, consultants and any other person who creates, receives, accesses, processes, stores or manages records on behalf of the Company.

It applies to information in electronic and physical form, including information held in:

- company databases and the TaxiTel management system;
- computers and authorised mobile devices;
- email and approved messaging systems;
- operational, dispatch and call-centre systems;
- accounting systems;
- cloud and backup systems;
- paper files, contracts and correspondence;
- vehicle and driver records; and
- any other approved information system.

SECTION 03

3 General Principles

3.1 Business purpose

Records are collected, created and retained only where there is a legitimate operational, contractual, financial, administrative, security or legal reason.

3.2 Accuracy

Employees responsible for company records must take reasonable steps to keep information accurate, complete and up to date.

3.3 Access control

Access to records is limited to employees and authorised persons who need the information for a legitimate business purpose. Sensitive information — including employee information, customer information, financial data, passwords, identification documents and confidential client information — receives additional protection.

3.4 Confidentiality

All personnel must keep confidential the records they can access, and must not disclose company, customer, employee, supplier or client information without authorisation.

3.5 Data minimisation

TaxiTel retains only information reasonably necessary for its operations, contractual and legal obligations, dispute management, security and legitimate business needs.

3.6 Secure storage

Records are kept in appropriate physical or electronic storage with reasonable technical and organisational safeguards.

SECTION 04

4 Roles and Responsibilities

Who	Responsibility
Managing Director	Approves this Policy and any significant exception to it.
Legal Department Manager	Owns this Policy; oversees its implementation; maintains the retention schedule; decides on legal holds and their release; approves disposal of records where required; advises staff; manages the response to any loss or breach of records.
Department managers	Ensure that records under their control are kept, stored and disposed of in line with this Policy.
IT function	Implements technical safeguards, access controls, backups, system security and secure deletion procedures for electronic records.

Who	Responsibility
Finance and administration	Maintain accounting, tax, procurement, contractual, employee and other administrative records in line with this Policy.
All employees and authorised users	File and store records correctly; prevent unauthorised access or disclosure; follow the retention periods; never destroy records subject to an investigation, audit, dispute or legal hold; report suspected loss, misuse or unauthorised disclosure.

SECTION 05

5 Records Classification

Classification	Description
Public	Information approved for public release.
Internal	Routine business information intended for use within TaxiTel.
Confidential	Information requiring restricted access, including contracts, financial information, internal reports, customer information and commercial information.
Highly confidential / restricted	Information requiring the highest level of protection, including passwords, identification documents, employee records, banking information, sensitive personal data, system credentials and security-related information.

Access is granted according to business need and authorisation level.

SECTION 06

6 Data Retention Schedule

Unless a longer period is required by applicable law, contract, audit, investigation, legal proceeding, donor or client requirement, TaxiTel applies the following retention periods:

Record category	Retention period
Company incorporation and ownership documents	Permanent
Licences, registrations and major corporate records	Permanent, or duration of validity plus 5 years
Financial statements and accounting records	5 years
Invoices, receipts and payment records	5 years

Record category	Retention period
Tax and statutory financial records	At least 5 years, or longer where legally required
Bank statements and financial transaction records	5 years
Customer and client contracts	5 years after expiry or termination
Supplier and subcontractor contracts	5 years after expiry or termination
Tender, quotation and procurement files	5 years
Employee personnel records	5 years after the end of employment
Payroll and employee payment records	5 years
Driver files and qualification records	5 years after the end of engagement
Vehicle registration, insurance and maintenance records	5 years after disposal or end of service
Trip, booking and dispatch records	5 years
Customer service and complaint records	5 years after closure
Accident and incident reports	5 years after the matter is closed
Insurance claims and related records	5 years after final settlement
Client contact information	Duration of the business relationship plus 5 years, unless earlier deletion is appropriate
Business correspondence of contractual significance	5 years
Audit and compliance reports	5 years
Gifts register and conflict-of-interest declarations	5 years
Training and policy acknowledgement records	Duration of employment plus 5 years

Record category	Retention period
Legal claims and dispute files	5 years after final resolution, or longer where advised
Internal policies and procedures	Current version, plus previous versions for at least 5 years
Call-centre operational records	3 years
Routine business correspondence	3 years
Quote requests and enquiries that do not lead to a booking	24 months
Unsuccessful job applications	12 months
Call recordings, where calls are recorded	Normally 12 months, unless needed for a complaint, investigation, contract or legal matter
IT system access and security logs	Normally 12 months
System backup copies	According to the backup cycle of our systems and providers
CCTV recordings, where applicable	Normally 30–90 days, unless needed for an incident or investigation

This schedule is TaxiTel's standard. Where a binding legal, contractual, donor or client requirement specifies a longer period, the longer period applies.

SECTION 07

7 Client and Passenger Information

TaxiTel processes information about passengers, client representatives, drivers, trip locations, telephone numbers, bookings, vehicle assignments and other operational information needed to provide transport services. This information:

- is used only for legitimate operational, contractual, safety, billing, reporting or legal purposes;
- is available only to authorised personnel;
- is not disclosed to third parties without an appropriate business, contractual or legal reason; and
- is deleted or anonymised when there is no longer a legitimate reason to keep it.

Where TaxiTel processes information on behalf of a client, the client's contractual retention and confidentiality requirements are also respected. Further detail is set out in the Privacy Policy (TT-POL-002).

SECTION 08

8 Electronic Records and Information Security

Electronic records are protected by security measures appropriate to the type of information. Controls may include:

- individual user accounts and strong passwords;
- role-based access restrictions;
- system logging;
- firewall and network controls;
- secure backups;
- anti-malware or endpoint protection;
- restricted administrator privileges;
- encryption where appropriate;
- physical security of equipment; and
- periodic access reviews.

Employees must not store sensitive company records on unauthorised personal devices, personal cloud-storage services or unapproved systems.

SECTION 09

9 Physical Records

Paper documents containing confidential or sensitive information are kept in secured areas. Access to sensitive personnel, financial, contractual and customer files is limited to authorised personnel. When physical documents are no longer required, they are destroyed in a way that prevents reconstruction or unauthorised disclosure, such as secure shredding.

SECTION 10

10 Backups

TaxiTel maintains appropriate backups of critical electronic systems and information to support business continuity and recovery. Backups are intended for disaster recovery and are not treated as permanent archival storage. Information deleted from active systems may remain temporarily in backup copies until those backups are overwritten or removed under the normal backup cycle.

SECTION 11

11 Legal Hold and Suspension of Deletion

Normal deletion or destruction of records is suspended where TaxiTel becomes aware that information may be relevant to:

- litigation or potential litigation;
- an investigation or audit;
- a regulatory or governmental request;
- an insurance claim;
- a contractual dispute;
- suspected fraud or misconduct; or
- any other matter requiring evidence to be preserved.

> **A legal hold overrides the retention schedule**
>
> Relevant records remain protected until the Legal Department Manager confirms in writing that the hold may be released.

SECTION 12

12 Secure Disposal

When the retention period has expired and there is no continuing business, contractual, legal or investigation requirement, records are securely destroyed, deleted or anonymised. Appropriate methods include:

- secure shredding of paper documents;
- secure deletion of electronic files and database records;
- secure wiping or destruction of storage devices before disposal; and
- anonymisation, where statistical information remains useful — for example, keeping trip totals while removing passenger names and phone numbers.

Records containing confidential information must never be thrown away with ordinary waste where the information could be recovered.

SECTION 13

13 Third Parties and Service Providers

Where TaxiTel uses third-party providers to process or store company information, reasonable steps are taken to ensure they maintain appropriate confidentiality and security. Where appropriate, contracts address confidentiality, authorised use of information, security, return or deletion of information, incident reporting, and compliance with contractual and legal requirements.

SECTION 14

14 Loss or Breach of Records

Any employee who becomes aware of lost records, unauthorised access, accidental disclosure, theft of records or equipment, suspicious system activity, or unauthorised deletion or alteration of information must report it promptly to their manager and to the Legal Department Manager. TaxiTel will investigate and take appropriate corrective measures, and will inform affected clients and partners where their contracts require it.

SECTION 15

15 Employee Departure and Change of Duties

When an employee, contractor or authorised user leaves TaxiTel or changes duties:

- their access rights are reviewed and withdrawn where appropriate;
- company documents and devices are returned;
- company information must not be kept or copied without authorisation; and
- responsibility for the records they managed is transferred to the appropriate department.

SECTION 16

16 Monitoring, Exceptions and Non-Compliance

The Legal Department Manager may review compliance with this Policy at any time. Any exception must be justified by an operational, contractual, regulatory, legal or security requirement, approved by the Legal Department Manager and, for significant exceptions, by the Managing Director.

Failure to comply with record-management, confidentiality or information-security requirements may lead to corrective or disciplinary action. Serious unauthorised disclosure, destruction, alteration or misuse of company records may also lead to contractual or legal action.

SECTION 17

17 Policy Review and Approval

This Policy is reviewed at least once a year by the Legal Department Manager, and sooner if there are significant changes to legal or client requirements, company operations, information systems, technology, contractual obligations or information-security risks.

Approval

This Records Management and Data Retention Policy is approved by TaxiTel and applies throughout the Company.

Name	______________	Title	______________
Signature	______________	Date	______________
Company stamp	______________		