FOXTROT

FX-POL-011

CORPORATE GOVERNANCE

Information Security & Data Protection Policy

Controls for company, client and personal data across devices, accounts, cloud services, subprocessors and incident response.

VERSION 1.0 · EFFECTIVE 15 SEPTEMBER 2026

DOCUMENT CONTROL

DOCUMENT	Information Security & Data Protection Policy
DOCUMENT REFERENCE	FX-POL-011
ISSUED BY	Foxtrot LLC, an Arizona limited liability company
VERSION	1.0
EFFECTIVE DATE	15 September 2026
APPROVED BY	Farshad Mohammadi, Managing Member
OWNER	Managing Member
REVIEW CYCLE	Annual, and after any security or privacy incident
APPLIES TO	All company and client information, all personal data processed by the company, and everyone who handles it on the company's behalf
RELATED DOCUMENTS	FX-POL-001, FX-POL-004 Responsible AI & AI Ethics Statement, FX-POL-005, FX-POL-009
CONTACT	compliance@foxtrotllc.com
CLASSIFICATION	Public. Provided to clients, suppliers, regulators and supplier registration portals

Contents

1 Purpose and scope 3
2 Accountability and frameworks 3
3 Information classification 3
4 Device and account controls 4
5 Working away from base 4
6 Client data, platform data and residency 4
7 Personal data 5
8 Subprocessors and third-party services 5
9 Backup, continuity and disposal 5
10 Incident response 6
11 Training and awareness 6
12 Monitoring and review 6
13 Approval 6
Revision history 7

1 Purpose and scope

Foxtrot LLC holds information that matters to other people: client maintenance records, fleet and transaction data, lease terms, inspection findings, and personal data about personnel, crew and client contacts. The Synops platform processes operational data on behalf of airline customers. This policy sets out how that information is protected and how personal data is handled.

It applies to all company and client information in any form, to all personal data the company processes as controller or as processor, and to everyone who handles it, including contractors and subcontractors. Suppliers carry equivalent obligations under FX-POL-005 Section 13.

2 Accountability and frameworks

The Managing Member is accountable for information security and data protection, including control decisions, subprocessor approval, breach notification, and this policy.

The company aligns its practice with the CIS Critical Security Controls implementation group 1 and with ISO/IEC 27001 as a management-system reference, and applies the principles of the GDPR, the Saudi Personal Data Protection Law, Canadian PIPEDA, and applicable United States state privacy law.

> ALIGNMENT IS NOT CERTIFICATION
>
> Foxtrot LLC does not hold ISO/IEC 27001, SOC 2, or any other security certification, and does not claim one. Where a client requires certified assurance, the company says so plainly and offers its controls, evidence and audit cooperation instead. Any certification obtained will be stated on foxtrotllc.com/policies with the certificate reference and date.

3 Information classification

CLASS	EXAMPLES	HANDLING
Client confidential	Maintenance records, fleet and utilisation data, inspection findings, lease and transaction terms, pricing, proprietary manuals	Encrypted storage, access limited to the engagement, never shared outside the engagement, returned or destroyed when required
Personal data	Personnel and contractor records, crew and client contact details, platform user accounts	Collected only as needed, lawful basis identified, access limited, retention limited
Company confidential	Commercial pipeline, contracts, pricing models, source code, product roadmap	Encrypted storage, access limited to those who need it
Public	Published policies, marketing material, website content	No restriction

Client and company confidential information is not placed in personal accounts, personal storage, consumer messaging apps, or any service the client has not been told about.

4 Device and account controls

- Full disk encryption on every device used for company or client data.
- Screen lock with a short timeout, and a strong unique passphrase on every device.
- Multi-factor authentication on every account that supports it, including email, cloud storage, code repositories, cloud infrastructure, and the company's own platform.
- A password manager for credentials, with no reuse of passwords across services and no credentials in documents, code, tickets or messages.
- Operating systems, browsers and applications kept current, with security updates applied promptly.
- Endpoint protection enabled, and remote wipe available on portable devices.
- Least privilege on cloud infrastructure and administrative accounts, with separate administrative credentials and no shared logins.
- Access reviewed at least annually and removed promptly on reassignment or departure, including third-party access.
- No use of unmanaged public computers or unsecured shared networks for client work, and a VPN where a network cannot be trusted.

5 Working away from base

Most of our work happens in hangars, offices and hotels that belong to someone else, which is where information is most often lost:

- devices are not left unattended in vehicles, hangars, crew rooms or hotel rooms;
- screens are positioned so that client data is not readable by others;
- photographs of aircraft, registrations, records and defects are taken only where the client has authorised it, are stored in company storage rather than in a personal camera roll, and are deleted from the device once transferred;
- paper records taken on site are minimised, kept in the person's possession, and scanned into company storage and then destroyed;
- client data is not discussed in public areas, on open radio channels, or in earshot of other parties to a transaction;
- loss or possible loss of a device is reported immediately, at any hour.

6 Client data, platform data and residency

For the Synops platform, customer data belongs to the customer. Tenants are logically segregated with access controls and encryption in transit and at rest. There is no cross-tenant learning or reuse. In-region deployment is available where residency is required. Models are not trained, fine-tuned or improved on customer data without specific written consent recorded for that customer. On termination, data is exported to the customer and deleted on the agreed schedule, with written confirmation. FX-POL-004 sets out the AI-specific commitments and the traceability of outputs.

For technical services engagements, client records received for a pre-purchase inspection, lease return or delivery are held only for the engagement and the period the contract or applicable regulation requires, and are then returned or destroyed with confirmation.

7 Personal data

The company processes personal data only where it has a lawful basis, keeps it to what is necessary, and does not use it for a new purpose without checking that basis again.

- **Personnel and contractors**: identity and age verification, right to work, qualifications and authorizations, engagement terms, payment details, training and safety records. Basis: contract and legal obligation. Retention: seven years after the engagement ends, consistent with our documentation obligations, other than medical and accommodation information which is kept separately and only as long as needed.
- **Client and supplier contacts**: name, employer, role, business contact details. Basis: legitimate interest in performing and administering the engagement.
- **Platform users**: account and audit data necessary for access control and traceability. Basis: the customer's instruction as processor, under the customer agreement.
- **Grievance reports**: as set out in FX-POL-009, kept separately, shared only with those who need it, retained seven years.

Personal data is not sold, is not used for profiling individuals, and is not transferred to a further processor or another jurisdiction without the controlling party's consent. Where the company acts as processor, it acts only on the customer's documented instructions.

Requests from individuals to access, correct, delete, restrict or port their personal data, or to object to processing, are sent to compliance@foxtrotllc.com and answered within 30 days. Where the company holds the data as processor for a customer, the request is passed to that customer without delay and the company assists in answering it.

8 Subprocessors and third-party services

Cloud, model, payment, accounting and communication providers used to deliver our services are selected on security, contractual confidentiality and data location. Each is bound by written terms, and those relevant to the Synops platform are disclosed on the trust page with advance notice of material change.

A third-party service is not introduced into client work without checking what it does with the data, whether it trains on submitted content, where it stores data, and whether it offers contractual confidentiality. AI services that train on submitted content, or that do not offer contractual confidentiality, are not used for client technical data, maintenance records, personal data or confidential information, as required by FX-POL-001.

9 Backup, continuity and disposal

Company and client data is backed up to encrypted storage, with restoration tested at least annually. Critical engagement records are recoverable independently of any single device.

Devices and media are securely wiped before disposal, resale or transfer, and paper is shredded. Client material is destroyed or returned as the contract requires, with written confirmation where asked.

10 Incident response

Any suspected loss, theft, unauthorised access, account compromise, malware, misdirected disclosure or ransomware is reported to the Managing Member immediately, at any hour. The response is:

1. contain: isolate the device or account, revoke sessions and credentials, and preserve logs and evidence;
2. assess: establish what data and whose data is affected, and whether personal data is involved;
3. notify: inform affected clients without delay, and in any event within 24 hours of establishing that their data is affected, and notify regulators and individuals where the law requires it and within the applicable deadline;
4. remediate: close the cause, restore from backup where needed, and confirm the system is clean;
5. record and review: log the incident, root cause, action taken and lessons, and change the control that failed.

Suppliers must report incidents affecting our data or client data within 24 hours under FX-POL-005 Section 13. The company does not condition support or payment on a supplier keeping a security incident quiet.

11 Training and awareness

Everyone who handles company or client data receives this policy at onboarding, confirms they have read it, and is briefed at least annually on device security, phishing and social engineering, handling client records on site, AI tool restrictions, and incident reporting. Completion is recorded.

12 Monitoring and review

The Managing Member reviews this policy and the controls in it at least once a year and after any incident. The review covers access rights, multi-factor coverage, patch status, backup restoration testing, subprocessor list, incidents and near misses, and any client or supplier assessment finding. Findings and actions are recorded and retained for at least seven years.

13 Approval

This policy is adopted on behalf of Foxtrot LLC and takes effect on the date shown on the cover of this document.

DocuSigned by:
Farshad Mohammadi
4620BECE0E724B4...

FARSHAD MOHAMMADI, MANAGING MEMBER

15 September 2026

DATE

Revision history

VERSION	DATE	SUMMARY OF CHANGE	APPROVED BY
1.0	15 September 2026	First issue. Replaces the generic references to an information security policy and a data processing statement previously made in FX-POL-004.	Farshad Mohammadi, Managing Member

Controlled electronically. The authoritative version is the one published at foxtrotllc.com/policies.