

Ordo Systems Security Overview

A concise customer view of principal safeguards and shared responsibilities.

Effective	08/2026
Version	1.0
Publisher	Shane Tharuka Sarathchandra Keeragala Dewage trading as Ordo Systems
Document	Customer-facing overview
URL	https://legal.ordosystems.com.au/security

1. Purpose and limitations

This Overview describes the principal safeguards designed for Ordo Systems’ web, mobile and backend service. It is informational and does not create a certification, warranty, service level, uptime commitment, recovery objective or guarantee that every security event can be prevented. Contractual commitments appear only in the Terms and an accepted Order Form.

2. Shared responsibility

Ordo Systems	Organisation and Users
Operates and secures the service platform; enforces authenticated access; manages service infrastructure, security processes and providers; investigates reported incidents.	Choose and review Administrators; manage Users, Departments and allocations; protect devices and credentials; enter lawful, necessary data; review reports and outputs; report suspected compromise.

3. Identity and access

- Organisation membership, role, Department, allocation and route capability are resolved by the server; client-supplied authority does not by itself grant access.
- Hosted signup uses recipient-controlled activation, a password and MFA before the Primary Admin becomes active.
- Primary Admin and Admin accounts require MFA. Selected privileged actions require a recently MFA-verified session.
- Password recovery does not automatically sign a User in and can revoke active sessions. Assisted MFA reset is restricted to eligible, MFA-verified administrative authority.
- Browser sessions use an HTTP-only, same-origin session cookie; native clients store a separate server-validated trusted-session credential through the platform’s secure-storage mechanism.
- Biometrics or an app passcode may unlock the trusted native session locally. Server validation, expiry and revocation still apply; invalid sessions require full reauthentication, and local unlock does not replace MFA.

4. Organisation and role separation

Protected requests derive the active Organisation from an authenticated session and active membership. Access to Fuel, Trade Plate, receipt-image, report and administrative records is checked against the Organisation, role,

Department or direct allocation and route capability. Developer diagnostics do not automatically grant customer-business-data access.

5. Data and file safeguards

- Production architecture requires PostgreSQL for structured data and private, S3-compatible object storage for receipt images, statements and generated files; development JSON and filesystem modes are not production authority.
- Production database connections require certificate-verified TLS, and custom object-storage endpoints must use HTTPS.
- Stored files use server-generated object identities. User filenames are metadata and do not decide access. Downloads require Ordo Systems authorisation and protected download controls.
- The supported Fuel workflow is designed for a fuel-card last-four value, not a full payment-card or fuel-card number. Customers must not enter a full number.
- Security and audit records are intended to use bounded, sanitised metadata and scoped access rather than secrets or unrestricted business content.

At-rest encryption, backup encryption, provider certifications and data-residency claims depend on the confirmed production providers and contracts and must be described only where separately verified.

6. Product-specific safeguards

Trade Plate secure-QR labels use an opaque random value rather than a readable plate number, Organisation, Department or internal record identifier. Resolution is online and server-authoritative; invalid, revoked and out-of-scope values receive a generic failure. The mobile workflow is designed to keep the scanned value in volatile runtime state and out of local storage and offline queues. Replacement and revocation are privileged, recently MFA-verified actions.

Initial QR issuance is governed by the then-current authorised service workflow. This Overview does not claim that every issuance action has the same recent-MFA control as replacement and revocation.

Receipt images and related records are scoped to the relevant Organisation and account. The current receipt-review stub does not process image bytes through an external production OCR provider and does not replace User review. Separate vehicle-registration recognition operates on-device using a temporary image that is deleted after processing.

7. Mobile and device controls

Mobile devices may hold a secure session credential, preferences, installation and sync state, and account-partitioned pending workflow data. Working data in browser/device storage should not be assumed to have the same protection as the secure credential. Receipt-image binaries are not persisted in mobile local storage. On packaged mobile clients, Trade Plate QR PNG and PDF exports use a temporary app-cache copy for the device save/share workflow, and Ordo Systems attempts to remove that copy after handoff.

The current build records server-side Trade Plate borrow and return times but does not capture device location. Authenticated in-app operational notifications are available within Ordo Systems; customer push notifications are postponed and are not part of the launch service. Camera and photo access are user-initiated for supported workflows. No advertising or behavioural-tracking SDK was identified in the reviewed build.

Users should protect devices, keep operating systems current, sync pending work, and clear local data and sign out before transferring a device. The Clear My Local Mobile Data action is not backend account deletion and does not itself end the session. Self-service account deletion is a separate, reauthenticated server-side process that disables the User's sign-in identity and access and revokes all active browser and trusted native sessions. Limited disabled attribution is retained where needed to preserve historical Organisation records, reconciliation, security and audit integrity.

8. Logging, monitoring and incident response

Ordo Systems records bounded authentication, administrative, onboarding, reporting, security and operational events for accountability, troubleshooting and abuse detection. Access to audit and diagnostic information is restricted by role and Organisation scope.

Ordo Systems maintains incident-assessment and recovery procedures for the approved production environment. Actual backup windows, recovery points and recovery times depend on that environment and are not contractual unless stated in an Order Form. Where an incident affects an Organisation, Ordo Systems will investigate, take proportionate containment steps and make notifications required by applicable law.

9. Customer security practices

- use individual accounts and never share passwords, MFA factors or recovery codes;
- review Primary Admin, Admin, Department and allocation access regularly;
- remove access promptly when a person changes role or leaves;
- protect devices with current security updates and a suitable passcode;
- do not enter full card numbers, secrets or unnecessary sensitive information;
- review reports, recognition results and secure-QR outcomes before acting; and
- report suspected compromise promptly without accessing data beyond your authority.

10. Security reporting and updates

Report a suspected vulnerability or security incident to support@ordosystems.com.au. Include only the information reasonably needed to investigate. Do not disrupt the service, access another Organisation's data, retain personal information unnecessarily or publish exploit details before Ordo Systems has had a reasonable opportunity to investigate.

Ordo Systems may update this Overview as safeguards, providers or service functions change. Once published, its version and effective date will identify the current customer-facing description.