

Ordo Systems Support Policy

What standard support covers, how requests are prioritised, and where the boundaries sit.

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

1. Purpose

This Policy explains the standard support available for Ordo Systems. It does not create a service-level agreement, guaranteed response or resolution time, uptime commitment, recovery objective or after-hours service. Any additional commitment must be stated in an accepted Order Form.

2. Contacting support

Support channels:

- Email: support@ordosystems.com.au
- Reserved support page: <https://legal.ordosystems.com.au/support>
- Published support hours: **Monday to Friday, 08:00 to 17:00 Melbourne local time (AEST/AEDT as applicable)**

Include the Organisation, affected User or workflow, device or platform, approximate time, steps already tried and any safe error message. If an Organisation-level change is requested, we may ask the Primary Admin or another authorised Admin to confirm it.

Keep support messages safe

Do not send passwords, MFA codes, recovery codes, session tokens, full payment-card or fuel-card numbers, raw secure Trade Plate QR values, or unredacted personal information that is not needed for diagnosis.

3. What standard support covers

- sign-in, MFA, trusted-device biometric or app-passcode access and session issues, invitations and account-recovery guidance;
- User, Department, role, product-allocation and Organisation business-size questions;
- Fuel Receipt and Trade Plate workflows, including Trade Plate QR export, download, save or share issues;
- receipt-image upload, synchronisation and retry issues;
- manual reports, exports and delivery functions enabled for the Organisation;
- in-app notification issues;
- suspected service defects or incidents; and
- routing privacy, access, correction, deletion and security requests to the appropriate process.

Automated monthly Trade Plate reporting is unavailable for the current launch. Automated Fuel reporting is supported only where expressly enabled and configured; it is not a general delivery commitment.

4. How requests are prioritised

Priority	Typical impact	Handling
Critical	Suspected cross-Organisation access, active compromise, material data loss, or widespread inability to use an essential service.	Triage first and escalate to security or incident response where indicated.
High	A major enabled workflow is unavailable with no reasonable workaround.	Investigate according to impact and available diagnostics.
Standard	A limited defect, account question or workflow issue with a workaround.	Handle in the normal support queue.
Request	Guidance, feedback, training or a proposed improvement.	Review for guidance or future product planning; no delivery promise.

Priority may change after investigation. Unless an Order Form states otherwise, any estimated response, workaround or resolution time is an estimate only.

5. Support boundaries

Standard support does not include:

- managing the Organisation's devices, networks, email systems or third-party accounts;
- accounting, tax, legal, employment, safety, privacy-compliance or regulatory advice;
- data entry, correction or routine administration the Organisation can perform;
- custom development, integrations, migrations, training or data repair unless agreed;
- support for modified, unsupported or obsolete devices, browsers or operating systems;
- restoring data outside the approved recovery process; or
- features that are disabled, proposed, in development or not part of the current service.

6. Organisation and User responsibilities

To help us support the service safely, Users and Organisations should:

- keep the app and supported operating system reasonably current;
- maintain suitable connectivity and device access;
- protect accounts and promptly remove access that is no longer needed;
- sync pending work before clearing, resetting or transferring a device;
- keep independent records where required for legal or operational reasons;
- use synthetic or redacted screenshots and logs where possible; and
- cooperate with reasonable, proportionate diagnostic and verification requests.

Ordo Systems may decline an unsafe attachment or request a safer transfer method. A support request does not authorise access to another Organisation's data or unrestricted access to a User's device.

7. Security, privacy and urgent matters

Report a suspected vulnerability, account compromise or cross-Organisation issue to support@ordosystems.com.au. Include only what is reasonably needed to investigate and do not disrupt the service or access data beyond your authority.

Users can delete their own account through the in-app self-service deletion flow. Privacy requests, complaints, Organisation-closure enquiries, or help with the deletion flow may be sent to support@ordosystems.com.au. Those matters follow the Privacy Policy and Data Retention and Deletion Policy, not ordinary defect prioritisation.

For an immediate threat to personal safety or a suspected crime, contact the appropriate emergency or law-enforcement service first.

8. Maintenance and incidents

Ordo Systems may perform maintenance or temporarily restrict a function while investigating a security, integrity or availability risk. Where practicable, affected Organisations will receive reasonable notice or an update by [email](#). Communications will avoid exposing sensitive investigation details.

9. Changes and contact

Ordo Systems may update this Policy as its supported service and operating model change. We will show the current version and effective date. A material reduction to contracted support is handled under the Terms or applicable Order Form.

Support: support@ordosystems.com.au