Security and Access Overview

For the owner or IT reviewer approving ROI-AI

Last reviewed July 30, 2026. Published at roiaione.com/trust

ROI-AI connects to two systems in your environment: your ERP, and one mailbox you designate for chargeback correspondence. What Roy can read and write in each is enumerated below, every credential is one you issue and can revoke without our involvement, and nothing is filed with a retailer without a release step you control.

This document contains nothing beyond what is published at roiaione.com/trust. It exists so you can review and forward it without visiting the site or taking a call.

Access scope

Your ERP

What Roy reads. Roy queries a defined set of ERP tables for the records a dispute needs: chargebacks and chargeback detail, invoices and invoice detail, purchase orders, pick tickets and packing detail, shipments, style and size master data, and customer master records. It does not browse your ERP; every query is scoped to a named table set.

What Roy writes. ROI-AI's ERP writes are limited to the chargeback records the dispute work touches, meaning creating the case in your ERP and recording its outcome, plus purchase orders for customers who buy order entry. Nothing else in your ERP is writable, and there is no delete path in any of these functions. The outer boundary is the permission set your IT team grants the login: if you want no writes at all, scope the login to read-only and none of the above can write.

Scoping the login is your call. We work from the credentials and permissions your IT team chooses to grant. If you want ROI-AI limited to SELECT on a named table set, or to a dedicated set of views, we will work within that grant. Customers have done both.

What Roy cannot access. Any module the dispute work does not require. No general or ad-hoc access to your database, and no access to your wider network, file shares, or workstations.

One mailbox you nominate

ROI-AI connects to a single mailbox that you designate for chargeback correspondence, using an application registration in your own Microsoft tenant that your admin consents to and can revoke at any time. We ask your IT team to apply a Microsoft Exchange application access policy so that the registration can reach only that one mailbox, even though the permission is tenant-scoped by design. ROI-AI reads chargeback correspondence and attachments from that mailbox and sends dispute correspondence from the address you choose. It does not touch any other mailbox, calendar, file, or Teams content.

The application access policy is applied by your own administrator, so it is a control you hold and

can verify, not one you have to take our word for.

Retailer vendor portals

Where a retailer requires portal filing, ROI-AI uses a vendor-portal login that you provide and control. It is used to retrieve your chargeback and deduction records and, for retailers where you have enabled it, to file the dispute. The credential is held as a reference in AWS Secrets Manager or encrypted at rest, is revocable by you at any time, and every portal login is recorded.

What ROI-AI never touches

- Bank accounts, routing numbers, ACH or wire details, and payment initiation of any kind
- Payroll, HR, and employee records
- Credit card data
- General access to your network, file shares, or workstations
- Any ERP module beyond the tables the dispute work requires

ROI-AI moves documents and dispute correspondence. It never moves money. Retailer-issued remittance advice and check and deduction detail are used as evidence only; no payment instruction is ever issued from them.

How the connection is constrained

How connections are made. Each customer's ERP connection is a separate, independently configured connection record. ROI-AI connects out to the endpoint your IT team specifies; we do not ask you to open your ERP to the public internet, and we do not install anything on your network beyond what an agreed integration requires.

How credentials are held. ERP and portal credentials are held in AWS Secrets Manager or encrypted at rest with envelope encryption, are referenced by name rather than embedded in code or configuration, and are scoped to your organization alone. No credential is shared across customers, and revoking the login you gave us cuts our access immediately.

Your documents. Chargeback notices, bills of lading, invoices, packing lists, and the dispute packets Roy assembles are stored in Amazon S3 in our own AWS account, encrypted at rest with AES-256 and with public access blocked at the bucket level. Access is over TLS. Where a document is shown in the portal, it is served through a short-lived signed link rather than a public URL.

Separation between customers. Each account is its own organization. Your identity and your organization are established from your verified sign-in, not from anything a browser can set, so a request cannot be redirected at another customer's data by tampering with it. Access within your organization is role-based, and we hold automated tests that specifically assert one organization cannot read another's cases.

Where your data goes, and whether Roy trains on it

Your documents and records stay in our AWS environment. When Roy reasons over a case, the specific content needed for that step is sent over an encrypted connection to a hosted large-language-model API and the response comes back. Nothing is uploaded into a model

provider's file store, no model is fine-tuned on your data, and your data is not pooled with any other customer's. Case records and Roy's working transcripts are stored in our own database, not the model provider's.

If you need this as a contractual commitment rather than a description of how the system is built, we will put it in writing in a data processing agreement.

Categories of third party we rely on. We list categories and purposes rather than vendor names. If your review requires the specific providers, ask your ROI-AI contact and we will supply them in writing.

- **Cloud hosting and storage** – runs the application and stores your documents and case records, encrypted at rest.
- **Identity and authentication** – verifies who is signing in to your organization's account.
- **Hosted large-language-model API** – performs the reasoning step on the specific case content Roy sends for that step.
- **Email transport** – carries dispute correspondence to and from the mailbox you nominate.

Nothing reaches a retailer without a release step

Auto-submission is off by default, for every customer and every deduction reason code. Roy assembles the dispute and the evidence packet, and it is released for filing only after a review step. Whether a given reason code is ever released automatically is a setting you turn on deliberately, reason code by reason code, and you can turn it back off. Roy is not a fully autonomous filer, and we do not describe it as one.

What we ask of your IT team

A database login to your ERP, scoped how you choose. So Roy can read the invoices, purchase orders, shipment records, and chargeback detail that a dispute has to cite. Does not include administrator rights, access to modules the dispute work does not use, or access to the host beyond the database endpoint.

Access to one mailbox you designate for chargeback correspondence. So Roy can pick up retailer chargeback notices and their attachments, and send the dispute from an address you choose. Does not include any other mailbox, calendar, files, or Teams. We ask you to apply an Exchange application access policy that pins the registration to that single mailbox.

A vendor-portal login, only for retailers that require portal filing. So Roy can retrieve your deduction records and, where you enable it, file the dispute in the retailer's portal. Does not include anything beyond your own vendor account, and is not needed at all for retailers handled over email.

Certifications

ROI-AI does not currently hold SOC 2, ISO 27001, HIPAA, or PCI DSS certification, and we will not imply otherwise. We are happy to complete your security questionnaire, walk your IT team through our architecture, and sign a data processing agreement.

We also make no uptime or availability commitment here, because we do not have a measured

service level to quote you. Any commitment we do make is contractual and lives in our master services agreement.

A vendor with no attestations should be assessed on what it actually does and on who it is. The controls above are the first half of that.

How you keep control, and how you revoke access

Every credential you give us, you can revoke. Revoking it cuts our access immediately, with no dependency on us.

1. Disable the database login your IT team issued. ERP reads stop at once.
2. Revoke the application registration's consent in your Microsoft tenant, or remove it from the Exchange application access policy. Mailbox access stops.
3. Change or disable the vendor-portal login you provided. Portal access stops.
4. Turn off auto-submission for any reason code where you enabled it, at any time, without contacting us.

None of these steps requires our cooperation or a support ticket. What happens to your data after termination is governed by our master services agreement and privacy policy; ask your ROI-AI contact and we will confirm the process in writing for your records.

Questions this document does not answer

If your review needs the specific ERP objects we query, the named third-party providers, a completed security questionnaire, or a data processing agreement, ask your ROI-AI contact and we will supply it in writing.

The current version of this document is always at **roiaione.com/trust**.