



LEGAL & TRUST CENTRE

Platform policy pack

Clear rules. Accountable data. Trusted work.

Effective July 24, 2026 | Version 2026.07.24

This combined policy pack protects visitors, applicants, customer organizations, authorized users, support personnel, and the independent data boundary of every tenant. The public web versions control if this PDF becomes outdated.

Privacy: privacy@restorecheckiq.ca | Security: security@restorecheckiq.ca | Legal: legal@restorecheckiq.ca



POLICY INDEX

One governed source of truth

Each policy carries the same effective date and version. Material updates should be reviewed, published, and recorded through the release process.

01	Privacy Policy	How personal information is collected, used, disclosed, protected, retained, and made available to you.
02	Terms of Service	The contract rules for accessing and using RestoreCheck IQ's website, platform, APIs, and mobile experience.
03	Cookie & Local Storage Policy	A transparent inventory of cookies, local storage, service workers, and offline data used by the Services.
04	Acceptable Use Policy	Rules that keep the platform, organizations, integrations, and data safe.
05	Security & Trust Statement	The operational safeguards and accountability boundaries designed into RestoreCheck IQ.
06	Data Retention & Deletion Policy	How active records, evidence, offline data, backups, legal holds, and closure requests are managed.
07	Data Processing Addendum	Baseline privacy and security terms for Customer Data processed to provide the Services.
08	Subprocessor Register	The provider categories and optional integrations that may process data when configured for production.
09	Automated Processing & Human Review Notice	How extraction, scoring, routing, forecasting, and customer-connected automation are governed.
10	Mobile Application End-User Licence	Additional terms for the installable PWA and future Apple or Android packages.
11	Accessibility Statement	Our commitment, current target, feedback path, and honest limits.
12	Copyright, Trademark & Intellectual Property Notice	Ownership and permitted use of the RestoreCheck IQ platform, logo, materials, and customer content.
13	Customer Support & Service Commitment	How support is requested, classified, accessed, measured, and kept separate from customer work.
14	Subscription, Billing & Cancellation Policy	The controlled signup, payment confirmation, activation, renewal, cancellation, and refund process.
15	Account & Data Deletion Request	A public route for requesting deletion, including the verification and retention process.



Privacy Policy

How personal information is collected, used, disclosed, protected, retained, and made available to you.

Effective July 24, 2026	Version 2026.07.24	Audience Visitors, applicants, customers, authorized users, mobile users, and support contacts
----------------------------	-----------------------	---

1. Our commitment and scope

RestoreCheck IQ ("RestoreCheck IQ", "we", "us", or "our") provides a multi-tenant workflow, evidence, quality-control, reporting, integration, and support platform for restoration organizations. This Privacy Policy applies to our website, web application, installable mobile experience, customer support services, and related communications (collectively, the "Services").

We use personal information only for identified, reasonable purposes and apply safeguards appropriate to its sensitivity. An organization that subscribes to the Services generally controls the project, claim, document, and workforce information it uploads; RestoreCheck IQ processes that information to provide the Services and according to the organization's instructions. We remain responsible for personal information under our control, including information handled by service providers.

2. Information we collect

- Account and identity information, such as name, business email, organization, job role, authentication status, and account preferences.
- Registration, subscription, and transaction information, such as selected plan, billing cycle, billing method, payment status, invoices, and transaction references. Full payment-card data should be processed by the configured payment provider, not stored by RestoreCheck IQ.
- Customer content that authorized users choose to provide, including projects, insurer or carrier requirements, claim references, property or loss details, documents, photos, invoices, comments, approvals, and quality-control records.
- Support information, including case subject, description, contact information, troubleshooting data, authorized diagnostic scope, staff notes, and resolution history.
- Technical and security information, including session and device signals, IP address or privacy-preserving derivatives, browser type, timestamps, authentication events, audit records, integration events, and error or performance diagnostics.
- Integration information, such as API key metadata, webhook destinations, and connection status for customer-enabled services. Secret credentials are protected and are not displayed after creation where the product says so.
- Mobile and offline information, including locally encrypted evidence queued for upload, sync status, and service-worker cache data. Device permissions are requested only when a feature requires them.
- Communications and consent records, including registration confirmations, privacy choices, policy versions accepted, and marketing consent where separately requested.



3. How information is collected

We collect information directly from visitors, applicants, customers, and authorized users; automatically when the Services are used; from an organization that provisions or manages an account; from customer-configured integrations; and from service providers supporting hosting, storage, security, communications, billing, or customer support.

Customers must have authority to provide personal information and customer content to the Services. They are responsible for giving appropriate notices and obtaining required consents from their personnel, clients, claimants, property owners, vendors, and other individuals whose information they submit.

4. Why we use information

- Provide, secure, authenticate, maintain, support, and improve the Services.
- Create and administer registration applications, subscriptions, workspaces, authorized users, permissions, and two-factor authentication.
- Store, organize, validate, compare, report on, and export customer-directed project and requirement information.
- Process payments, maintain business records, and communicate service, security, billing, and support notices.
- Detect, investigate, prevent, and respond to fraud, abuse, security incidents, service failures, and violations of our agreements.
- Maintain tenant separation, access records, backup integrity, retention controls, legal holds, and disaster-recovery capability.
- Understand product reliability and workflow effectiveness using minimized, aggregated, or de-identified operational information where reasonably possible.
- Comply with law, enforce agreements, establish or defend legal claims, and protect people, customers, RestoreCheck IQ, and the public.

5. Consent and choices

Where consent is required, we seek meaningful consent in a form appropriate to the sensitivity and reasonable expectations involved. Core processing needed to provide a customer-requested Service is not presented as optional. Optional marketing, non-essential tracking, or materially new uses require an appropriate choice before they are enabled.

You may withdraw consent for consent-based processing, subject to legal or contractual restrictions and reasonable notice, by contacting privacy@restorecheckiq.ca. Withdrawal may prevent us from providing a feature that depends on that information.

6. When information is disclosed

We do not sell personal information and do not use customer project content for third-party advertising. Platform administrators do not receive routine access to customer project or document content. Any exceptional diagnostic access must be authorized, purpose-limited, time-bound, and auditable.

- To the customer organization and its authorized users according to configured roles and permissions.
- To vetted service providers that perform hosting, private object storage, database, email, billing, monitoring, security, or customer-authorized integration functions under contractual and confidentiality obligations.
- To a customer-selected integration or destination when an authorized user directs the transfer.



- To professional advisers, auditors, insurers, financing sources, or transaction counterparties subject to appropriate confidentiality and necessity controls.
- To law-enforcement, regulators, courts, or other parties where required or permitted by law, or where reasonably necessary to protect rights, safety, security, or service integrity.
- In connection with a merger, financing, reorganization, sale, or transfer, subject to lawful safeguards and notice where required.

7. International and interprovincial processing

Information may be processed in Canada or another country where an approved service provider operates. Information in another jurisdiction may be accessible to courts, law-enforcement, or national-security authorities under that jurisdiction's laws. Before production launch, the current subprocessor register and hosting regions must be published in the Trust Centre. Customers with residency requirements should contact us before uploading regulated data.

Where Quebec requirements apply, we assess privacy factors before communicating personal information outside Quebec as required by law.

8. Retention and deletion

We retain personal information only as long as reasonably necessary for the identified purposes, customer instructions, security, dispute resolution, and legal obligations. Customer administrators may configure eligible evidence-retention periods. A legal hold, investigation, backup cycle, or statutory requirement may temporarily delay deletion.

Encrypted offline evidence is designed to expire from the local queue after a limited period. Deleting an account or workspace does not mean every backup copy disappears instantly; residual copies are isolated from ordinary use and removed through the backup lifecycle unless preservation is required.

To request access, correction, export, or deletion, use available account controls or contact privacy@restorecheckiq.ca. We will verify identity and authority before acting.

9. Safeguards and incidents

Our safeguards are designed to include tenant-scoped authorization, role-based access, two-factor authentication for privileged access, encryption in transit, private object storage, encrypted offline queues, managed secrets, audit records, backup controls, secure development checks, and monitored incident response. No system can be guaranteed perfectly secure.

We investigate suspected confidentiality or security incidents, take reasonable steps to contain risk and prevent recurrence, maintain required records, and notify affected individuals, customers, and regulators when applicable law requires it.

10. Access, correction, complaints, and privacy rights

Subject to applicable law, you may ask about the existence, use, or disclosure of personal information under our control; request access or correction; challenge compliance; or ask about retention and authorized access. Contact the Privacy Officer at privacy@restorecheckiq.ca.

If information was provided through your employer or another customer organization, we may direct the request to that organization when it controls the information. We will explain any lawful limitation on access and provide available complaint or regulator information.



11. Children

The Services are business tools and are not directed to children. Individuals must be legally capable of using the Services for their organization. Do not submit information about a child unless the customer has a lawful, necessary business purpose and all required authority, notice, consent, and safeguards.

12. Changes and contact

We may update this Policy to reflect changes in law, technology, or our practices. We will post the new version and effective date and provide additional notice or obtain consent where required for a material change. Privacy Officer: privacy@restorecheckiq.ca. Legal notices: legal@restorecheckiq.ca. Registered office: Canada.



Terms of Service

The contract rules for accessing and using RestoreCheck IQ's website, platform, APIs, and mobile experience.

Effective July 24, 2026	Version 2026.07.24	Audience Customer organizations, authorized users, applicants, and website visitors
----------------------------	-----------------------	--

1. Agreement and authority

These Terms of Service ("Terms") form a binding agreement between RestoreCheck IQ and the person or organization using the Services. If you use the Services for an organization, you confirm that you have authority to bind it. "Customer" means the organization identified in an order, approved registration, or account; "Authorized User" means a person the Customer permits to use its workspace.

An order form, data processing addendum, or written enterprise agreement may add to these Terms. If there is a conflict, the signed enterprise agreement controls, followed by the order form, data processing addendum, and these Terms.

2. Eligibility and controlled activation

The Services are intended for lawful business use by persons capable of entering a binding agreement. A public registration is an application, not an active account. Access begins only after RestoreCheck IQ approves the application, verifies the applicable subscription or payment state, and the invited user completes secure activation.

Customers must provide accurate information, promptly update it, designate authorized administrators, and prevent shared or unauthorized credentials. Administrators control user access within their organization but cannot grant platform-owner authority.

3. Licence and acceptable use

During the subscription term and subject to payment and these Terms, RestoreCheck IQ grants the Customer a limited, non-exclusive, non-transferable right for Authorized Users to access the Services for the Customer's internal business operations.

Users must follow the Acceptable Use Policy. They must not attempt cross-tenant access, bypass security, introduce malicious code, overload the Services, misuse API credentials, reverse engineer protected elements except where law cannot prohibit it, or use the Services unlawfully.

4. Customer data and responsibilities

As between the parties, the Customer retains ownership of Customer Data. The Customer grants RestoreCheck IQ and its service providers a limited right to host, copy, transmit, display, and otherwise process Customer Data only to provide, secure, support, and lawfully operate the Services.

The Customer is responsible for the legality, quality, accuracy, permissions, retention settings, and instructions associated with Customer Data. The Customer must not upload data it lacks authority to use, and must not treat a platform score, extraction, forecast, report, or automated suggestion as a substitute for qualified human review.



5. Accuracy and professional judgment

RestoreCheck IQ is a workflow and decision-support system. It is not an insurer, engineer, lawyer, accountant, safety professional, or claims adjudicator. Carrier requirements, document extraction, calculations, alerts, quality-control checks, and forecasts depend on the source data, configuration, and review process.

The Customer must verify material outputs against original records and applicable requirements before relying on them. RestoreCheck IQ does not promise that every defect, omission, fraud indicator, compliance issue, or risk will be detected.

6. Fees, billing, taxes, and renewal

Fees, billing cycle, included usage, renewal, and payment method are stated in the applicable order or subscription confirmation. Unless the order says otherwise, fees are in Canadian dollars, exclusive of taxes, and non-cancellable and non-refundable after a paid service period begins except where law requires or RestoreCheck IQ expressly agrees.

Overdue undisputed amounts may result in restricted access after reasonable notice. We will not delete Customer Data merely because payment is late; suspension, export, retention, and termination follow the documented account process.

7. Security and account protection

Customers must use strong unique passwords, complete required two-factor authentication, protect devices and API credentials, maintain current contacts, and promptly report suspected compromise. Customers are responsible for activity under properly authenticated accounts unless caused by RestoreCheck IQ's breach of its obligations.

Security reports should be sent promptly to security@restorecheckiq.ca. Do not publicly disclose a suspected vulnerability before coordinated review where lawful.

8. Third-party services and APIs

Customer-enabled integrations, third-party applications, app stores, and external destinations are governed by their own terms and privacy practices. RestoreCheck IQ is not responsible for a third party's service, but remains responsible for its own selection and oversight of subprocessors as required by applicable law and contract.

API use is subject to authentication, tenant scope, rate limits, documentation, and the Acceptable Use Policy. Customers must ensure that any automation or AI system they connect cannot reuse credentials across organizations, broaden its data scope, or take unreviewed high-impact actions.

9. Confidentiality

Each party must protect the other party's non-public business, technical, security, and customer information using at least reasonable care, use it only for the agreement, and disclose it only to personnel and providers who need it and are bound to protect it. Standard exclusions apply to information that is public without breach, already lawfully known, independently developed, or lawfully received without duty.

A legally compelled recipient may disclose required information, but should give advance notice where lawful and reasonably assist protective efforts.

10. Intellectual property

RestoreCheck IQ and its licensors own the Services, software, designs, documentation, methods, reports templates, and trademarks, excluding Customer Data. "RestoreCheck IQ", the Proof Grid logo, and "Control. Verify. Improve." are claimed as trademarks of RestoreCheck IQ. No rights are granted except those expressly stated.



If a user provides feedback, RestoreCheck IQ may use it without restriction or payment, provided it does not identify the Customer or disclose Customer Confidential Information.

11. Service changes, availability, and support

We may improve or change the Services while seeking to preserve material subscribed functionality. Planned updates use migration, backup, rollback, compatibility, and verification controls intended to protect customer data. Emergency maintenance may occur without advance notice.

Unless a signed order includes a service-level agreement, support targets and availability information are operational objectives, not guarantees. Preview, beta, demonstration, and free features may be changed or withdrawn.

12. Suspension and termination

We may suspend access where reasonably necessary to address a security threat, unlawful use, material breach, or overdue payment, using the narrowest practical scope and notice where circumstances permit. Either party may terminate for uncured material breach after reasonable written notice, or as provided in an order.

On termination, Customer access ends. Subject to payment, law, security, and the agreed retention period, the Customer may request an available export before deletion. Confidentiality, payment, ownership, disclaimers, liability limits, and provisions intended to survive will survive.

13. Disclaimers

To the maximum extent permitted by law, the Services are provided "as is" and "as available". RestoreCheck IQ disclaims implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement. We do not warrant uninterrupted or error-free operation, complete detection, or that outputs will satisfy every carrier, regulator, contract, or customer requirement.

Nothing in these Terms excludes a warranty or remedy that applicable law does not permit the parties to exclude.

14. Limitation of liability

To the maximum extent permitted by law, neither party is liable for indirect, incidental, special, exemplary, punitive, or consequential damages, or lost profits, revenue, goodwill, or data, arising from the Services, even if advised of the possibility.

Except for payment obligations, misuse of the other party's intellectual property, breach of confidentiality, fraud, wilful misconduct, or liability that cannot lawfully be limited, each party's aggregate liability arising from the Services will not exceed the fees paid or payable for the affected Services during the twelve months before the event giving rise to the claim. These allocations are an essential basis of the agreement and require Canadian counsel confirmation for the Customer's contracting jurisdiction.

15. Governing law and disputes

The parties will first try in good faith to resolve a dispute through senior representatives. Unless a signed agreement specifies otherwise, these Terms are governed by the federal laws of Canada and the laws of the province or territory in which RestoreCheck IQ's registered office is located, without regard to conflict rules. Courts located in that jurisdiction have exclusive jurisdiction, except that either party may seek urgent injunctive relief in a competent court.

Consumer rights and mandatory local laws, if applicable, are not displaced.



16. General and contact

Neither party may assign the agreement without consent, except in a corporate reorganization or sale of substantially all related assets, subject to the successor assuming the obligations. Neither party is liable for delay caused by events beyond reasonable control. If a provision is unenforceable, it will be limited to the minimum extent necessary and the remainder continues. Notices may be electronic. Legal contact: legal@restorecheckiq.ca.



Cookie & Local Storage Policy

A transparent inventory of cookies, local storage, service workers, and offline data used by the Services.

Effective July 24, 2026	Version 2026.07.24	Audience Website, web application, and installable mobile users
----------------------------	-----------------------	--

1. Current position

RestoreCheck IQ currently uses cookies and browser storage that are necessary for authentication, security, integration hand-offs, preferences, installation, offline operation, and reliable delivery. We do not currently use third-party advertising cookies or behavioural advertising trackers.

If non-essential analytics or marketing technology is introduced, we will update this Policy and provide a consent choice before using it where required.

2. Technologies we use

- Session cookie: an HttpOnly, secure production cookie used to keep an authenticated user signed in. It is not available to ordinary page scripts.
- Two-factor and activation state: short-lived server-side records and request state used to complete secure account access.
- Integration state cookies: short-lived, same-site values used to verify an OAuth connection response and prevent request forgery.
- Authorized "view as" state: a short-lived, privileged cookie used to identify an explicitly selected organization during an audited platform-owner diagnostic session.
- Local storage: preferences such as dismissed notices or interface state. It must not contain reusable passwords, API secrets, or unencrypted customer evidence.
- IndexedDB/offline queue: customer-selected field evidence may be encrypted locally before later upload. Entries are scoped to the authenticated user and organization and expire under the offline retention rules.
- Service worker and cache storage: application shell assets used for installation, performance, and limited offline operation. Protected API responses and customer documents must not be persistently cached as public assets.

3. Control and consequences

Browsers and devices allow you to clear or block cookies and stored data. Blocking strictly necessary storage may prevent sign-in, integration connections, offline sync, or other core functions. Signing out clears the server session cookie; users should also remove local app data before transferring or disposing of a device.

Questions may be sent to privacy@restorecheckiq.ca.



Acceptable Use Policy

Rules that keep the platform, organizations, integrations, and data safe.

Effective July 24, 2026	Version 2026.07.24	Audience Customers, users, API clients, integration partners, and visitors
----------------------------	-----------------------	---

1. Use the Services lawfully and safely

You may use the Services only for lawful, authorized business purposes and within your assigned organization, role, subscription, documented API scope, and technical limits.

2. Prohibited activity

- Accessing, testing, enumerating, exporting, modifying, or attempting to discover another organization's data or identifiers without express written authorization from RestoreCheck IQ and the affected customer.
- Circumventing authentication, two-factor controls, role checks, rate limits, tenant scope, audit logging, retention controls, or other security measures.
- Sharing credentials, API keys, authenticator seeds, activation links, or recovery information; embedding platform-owner credentials in an organization automation; or using credentials after authorization ends.
- Uploading malware, unlawful content, information obtained without authority, or data that creates disproportionate risk without an agreed safeguard plan.
- Using the Services to harass, discriminate, defraud, mislead, surveil unlawfully, infringe rights, interfere with claims, or make unlawful automated decisions.
- Scanning, penetration testing, load testing, reverse engineering, scraping, or vulnerability exploitation without prior written authorization and a defined safe scope.
- Disrupting availability, sending abusive traffic, bypassing usage controls, or using the Services to operate competing hosted functionality.
- Removing proprietary notices, misrepresenting platform outputs as independently certified, or using the marks in a way that suggests endorsement.
- Connecting an AI or automated agent that has broader access than its human sponsor, mixes tenant data, retains data outside approved systems, trains on Customer Data without authority, or executes high-impact actions without human approval.

3. Enforcement and reporting

We may investigate suspected violations, preserve relevant evidence, restrict a token or account, or suspend the minimum necessary access. We will consider severity, intent, recurrence, customer impact, legal duties, and opportunities to cure. Illegal or dangerous activity may be reported where required or appropriate.

Report abuse to security@restorecheckiq.ca. Good-faith security research must be authorized before testing production.



Security & Trust Statement

The operational safeguards and accountability boundaries designed into RestoreCheck IQ.

Effective July 24, 2026	Version 2026.07.24	Audience Customers, security reviewers, procurement teams, and users
----------------------------	-----------------------	---

1. Security principles

- Tenant isolation: customer records and API operations are scoped to an organization; production PostgreSQL row-level security is an additional required defence.
- Least privilege: organization roles, separate platform roles, and a dedicated support workspace limit access to what a job requires.
- Privileged accountability: platform-owner and support activity is purpose-limited, time-bound where appropriate, and recorded.
- Strong authentication: permanent passwords, one-time activation, authenticator-based 2FA for privileged access, and protected session cookies.
- Private evidence: private object storage, signed delivery, encryption in transit, and encrypted offline evidence queues.
- Safe change management: additive migrations, staging rehearsal, backup and restore drills, rollback planning, compatibility checks, and release verification.
- Secret protection: production credentials belong in a managed secret provider, not source code, browser storage, logs, or downloadable reports.
- Data minimization: platform business intelligence and support operations exclude customer project content unless a separately authorized diagnostic need exists.

2. Security operations

RestoreCheck IQ maintains or plans production-owned controls for monitoring, alerting, vulnerability management, dependency review, backup restoration, retention, incident response, and independent testing. A control is not represented as certified or complete merely because supporting code exists; current production evidence governs.

Customers remain responsible for user lifecycle management, accurate permissions, secure devices, lawful uploads, integration configuration, and promptly removing access that is no longer required.

3. Vulnerability and incident reporting

Report suspected vulnerabilities or security incidents to security@restorecheckiq.ca with the affected feature, time, observed behaviour, and safe reproduction details. Do not include live credentials or unnecessary personal information. We ask reporters to avoid data access, persistence, disruption, extortion, and public disclosure before coordinated review.

No internet service can promise absolute security. This Statement describes control design and commitments; it is not a certification, penetration-test result, or guarantee.



Data Retention & Deletion Policy

How active records, evidence, offline data, backups, legal holds, and closure requests are managed.

Effective July 24, 2026	Version 2026.07.24	Audience Customers, privacy teams, records managers, and users
----------------------------	-----------------------	---

1. Retention principles

Information is kept only for a defined operational, contractual, security, dispute, or legal purpose. Retention is based on data type, sensitivity, customer configuration, legal obligations, backup lifecycle, and whether an active legal hold applies.

Deletion is designed as an accountable lifecycle, not an unlogged immediate database operation. Access may be suspended first, a recoverable closure window may apply, eligible objects are deleted, and residual backups age out under the backup schedule.

2. Working schedule

- Customer project and evidence records: for the subscription term and the customer-configured retention period; the current default may be seven years where the customer has not selected another lawful period.
- Encrypted offline evidence: only until successful upload or the short offline expiry period, currently designed not to exceed seven days.
- Authentication, security, and audit records: for the period reasonably needed to investigate activity, demonstrate accountability, prevent abuse, and meet legal duties.
- Support cases: for the active relationship and a reasonable post-resolution period needed for continuity, quality review, disputes, and security.
- Registration applications: while under review and for a reasonable period afterward to document the decision, prevent duplicate applications, and meet business or legal record duties.
- Billing and tax records: for the statutory period applicable to the transaction and RestoreCheck IQ's records.
- Backups: encrypted and access-restricted until rotation; they are not restored for ordinary access after a verified deletion except for disaster recovery, security, or legal necessity.
- Legal hold: overrides ordinary deletion only for the scope and duration reasonably required, with release and disposition recorded.

3. Requests and verification

Authorized administrators and individuals may request export, correction, account deletion, or workspace closure through account controls, support, or privacy@restorecheckiq.ca. We verify identity, organizational authority, and legal restrictions before acting.

Where a customer controls the information, individual requests may be referred to that customer. We will explain any required retention and delete or de-identify the remainder when the reason for retention ends.



Data Processing Addendum

Baseline privacy and security terms for Customer Data processed to provide the Services.

Effective July 24, 2026	Version 2026.07.24	Audience Customer legal, privacy, security, and procurement teams
----------------------------	-----------------------	--

1. Application and roles

This Data Processing Addendum ("DPA") forms part of the agreement between the Customer and RestoreCheck IQ when RestoreCheck IQ processes personal information in Customer Data on the Customer's behalf. The Customer is the organization that determines the business purposes and instructions; RestoreCheck IQ is its service provider or processor for that data. Each party remains independently responsible for personal information it controls for account, billing, security, legal, or business-administration purposes.

Terms such as controller, processor, service provider, personal information, and processing have the meaning given by applicable privacy law. The agreement, product configuration, and documented support instructions constitute the Customer's processing instructions.

2. Processing details

- Subject matter: hosting and operating a restoration workflow, evidence, requirement, QC, reporting, integration, and support platform.
- Duration: the subscription term plus the agreed export, retention, deletion, backup, and legal-hold periods.
- Nature and purpose: collection, storage, organization, comparison, validation, display, transmission, export, backup, support, security, and customer-directed deletion.
- People: Customer personnel, clients, claimants, property occupants or owners, contractors, vendors, insurer or carrier contacts, and others represented in Customer Data.
- Data: identity and contact information, project and claim context, property and loss details, documents, photos, invoices, comments, requirements, workflow decisions, audit records, and other data the Customer chooses to provide.
- Sensitive data: may be present in evidence or claim materials. Customers must minimize it, restrict it, and obtain written agreement before intentionally using the Services for special categories that require controls not documented in the order.

3. RestoreCheck IQ obligations

- Process Customer Personal Information only on documented instructions, unless law requires otherwise.
- Ensure personnel with access are authorized, trained, subject to confidentiality, and limited by role and need.
- Maintain safeguards appropriate to sensitivity and risk, including tenant scope, access control, auditability, encryption, backup, secure change management, and incident response.
- Notify the Customer without undue delay after confirming a breach of security safeguards affecting Customer Personal Information, and provide reasonably available information needed for the Customer's obligations.
- Assist reasonably with access, correction, deletion, privacy-impact, security, audit, and regulator requests, considering the nature of processing and information available.



- Delete or return Customer Personal Information at the end of Services as agreed, unless law requires retention.
- Make information reasonably necessary to demonstrate these obligations available, subject to confidentiality, security, proportionality, and protection of other customers.

4. Customer obligations

The Customer will provide lawful instructions, establish a valid authority for processing, deliver required notices, obtain required consent, configure appropriate access and retention, respond to people whose data it controls, and avoid uploading information not necessary for its business purpose.

The Customer will review source documents and material outputs, secure its users and integrations, and promptly notify RestoreCheck IQ of suspected unauthorized access or unlawful instructions.

5. Subprocessors and transfers

The Customer generally authorizes the subprocessors listed in the current Subprocessor Register for the described functions. RestoreCheck IQ will require appropriate data protection and confidentiality terms, remain responsible for its subprocessor obligations as required by law and contract, and provide notice of material additions where the agreement requires it.

Cross-border processing will use legally appropriate safeguards and privacy assessment where required. The Customer must identify binding residency restrictions before production use.

6. Audit, conflict, and signatures

We will first satisfy reasonable assurance requests using current policies, control descriptions, independent reports, and written responses. On-site review is reserved for a material unresolved concern or legal requirement and must protect security and other customers.

This DPA is a baseline template and becomes binding only as part of an accepted service agreement or signed order. Jurisdiction-specific schedules may be required. Contact legal@restorecheckiq.ca.



Subprocessor Register

The provider categories and optional integrations that may process data when configured for production.

Effective July 24, 2026	Version 2026.07.24	Audience Customers, privacy teams, security reviewers, and procurement teams
----------------------------	-----------------------	---

1. Important deployment status

This register distinguishes required production providers from optional customer-enabled integrations. A provider must not be represented as active until its production contract, region, security review, and data-processing terms are confirmed. The final provider legal name, processing region, and effective date must be completed before public production launch.

Not every provider receives every category of data. RestoreCheck IQ applies necessity, least privilege, contractual safeguards, and customer configuration.

2. Core provider categories

- Cloud application hosting and content delivery: application code, request metadata, and encrypted traffic.
- Managed PostgreSQL database: account, organization, workflow, audit, support, and configuration records.
- Private object storage: customer-uploaded documents, photos, generated reports, and evidence objects.
- Transactional email: recipient address and the minimum content needed for activation, security, billing, and support messages.
- Billing and payment processing: customer, subscription, invoice, transaction, and payment-token information.
- Monitoring and incident response: minimized error, performance, release, and security telemetry; customer document contents should be excluded.

3. Optional integrations

- QuickBooks/Intuit: only when an authorized customer connects accounting sync.
- Twilio or another messaging provider: only when the customer enables SMS notifications.
- Slack or customer webhooks: only for destinations configured by an authorized customer administrator.
- OCR or document-processing provider: only if enabled and disclosed for the affected workflow; source documents must not be used to train a provider model without separate lawful authority.
- Apple and Google distribution services: app-store account, device, diagnostic, purchase, or distribution information governed by the applicable store.

4. Changes and objections

We will update this page before a new material subprocessor begins processing Customer Personal Information and provide contractual notice where required. Customers may raise a reasonable data-protection objection at privacy@restorecheckiq.ca; the parties will work in good faith on a practical alternative.



Automated Processing & Human Review Notice

How extraction, scoring, routing, forecasting, and customer-connected automation are governed.

Effective July 24, 2026	Version 2026.07.24	Audience Customers, reviewers, administrators, API users, and affected individuals
----------------------------	-----------------------	---

1. Decision-support, not autonomous authority

RestoreCheck IQ may use deterministic rules, parsing, calculation, OCR, workflow automation, classification, or forecasting to organize information and identify items for review. These tools support human decisions; they do not approve claims, determine insurance coverage, establish legal compliance, replace source documents, or make employment decisions on RestoreCheck IQ's behalf.

A confidence indicator is not proof of correctness. Material requirements, calculations, matches, exceptions, risk scores, and exports must remain traceable to source data and reviewable by an authorized person.

2. Accuracy and improvement controls

- Preserve the source document beside extracted requirements so reviewers can compare the output.
- Use explainable rules, versioned requirement sets, confidence, validation failures, and human approval states.
- Separate training, test, demo, and production data; never use one customer's identifiable data to improve another customer's output without lawful authority.
- Measure extraction and workflow performance against a representative regression corpus before release.
- Record corrections in a tenant-scoped feedback history and promote rule changes only after review and regression testing.
- Provide an override, correction, escalation, or appeal path for consequential outputs.

3. Customer-connected AI and agents

A customer may connect its own AI or automation only through approved tenant-scoped credentials and documented API permissions. It must not receive platform-admin access, reuse credentials across organizations, train on data beyond the customer's authority, or execute destructive or high-impact actions without an explicit human control.

RestoreCheck IQ does not enable platform-wide AI processing merely because one customer connects an AI tool. The connecting customer is responsible for that provider's notices, consent, retention, security, output review, and lawful use.



Mobile Application End-User Licence

Additional terms for the installable PWA and future Apple or Android packages.

Effective July 24, 2026	Version 2026.07.24	Audience Mobile and tablet users
----------------------------	-----------------------	-------------------------------------

1. Licence and account

Subject to the Terms of Service, RestoreCheck IQ grants an Authorized User a limited, revocable, non-exclusive, non-transferable licence to install and use the mobile application on devices the user owns or controls for the Customer's internal business.

The mobile application is currently delivered as an installable, phone-first progressive web application. Native iOS or Android packages, if distributed, may include additional app-store terms.

2. Device and offline responsibilities

- Protect the device with a current operating system, screen lock, secure account, and remote-loss controls where available.
- Do not share an authenticated device or leave it unattended; sign out and remove local app data before device transfer or disposal.
- Offline evidence may be encrypted on the device until upload. Users must confirm sync before relying on the server record and must not clear app storage while evidence is pending.
- Camera, file, notification, and other permissions are requested only for the selected feature and can be changed in device settings, although a feature may stop working.
- Do not circumvent platform updates, certificate checks, device protections, or organization mobile-security requirements.

3. Stores, updates, and support

Apple, Google, and device manufacturers are not responsible for the Services except to the extent their mandatory terms state otherwise. RestoreCheck IQ, not an app store, is responsible for product support and privacy commitments.

Updates may be required for security, compatibility, and data integrity. Release controls are designed to preserve server records and pending mobile evidence, but users should complete or verify critical sync before planned maintenance where notified.

Mobile support: support@restorecheckiq.ca. Privacy: privacy@restorecheckiq.ca.



Accessibility Statement

Our commitment, current target, feedback path, and honest limits.

Effective July 24, 2026	Version 2026.07.24	Audience All visitors and users
----------------------------	-----------------------	------------------------------------

1. Commitment and target

RestoreCheck IQ is committed to making the Services usable by people with disabilities. Our product target is WCAG 2.2 Level AA across supported responsive web and mobile experiences. This is a development target, not a claim of independently audited conformance.

We work toward semantic structure, keyboard operation, visible focus, sufficient contrast, reduced-motion support, readable scaling, labelled controls, useful error messages, and layouts that reflow without overlap.

2. Known considerations

Customer-uploaded documents, generated files, third-party integrations, and legacy screens may not always meet the same level. Complex charts should include underlying data or an equivalent text explanation. Accessibility must be tested at full-page level and at supported responsive sizes.

We prioritize barriers that prevent sign-in, navigation, evidence capture, quality review, support, privacy choices, or account control.

3. Feedback and accommodation

If you encounter a barrier, contact support@restorecheckiq.ca with the page or feature, device, browser, assistive technology, and the task you were trying to complete. Do not include passwords or unnecessary personal information. We will acknowledge the report and work toward an accessible alternative.

Customers may request policy documents in an alternate format. Timing will depend on the format and complexity, and we will communicate progress.



Copyright, Trademark & Intellectual Property Notice

Ownership and permitted use of the RestoreCheck IQ platform, logo, materials, and customer content.

Effective July 24, 2026	Version 2026.07.24	Audience Visitors, customers, partners, media, and users
----------------------------	-----------------------	---

1. RestoreCheck IQ property

The Services, source and object code, product architecture, user interface, documentation, visual designs, report templates, graphics, text, and other materials created by or for RestoreCheck IQ are protected by copyright, trademark, and other intellectual-property laws.

RestoreCheck IQ(TM), the Proof Grid logo, and Control. Verify. Improve.(TM) are trademarks claimed by RestoreCheck IQ. The (TM) symbol indicates a trademark claim; it does not represent that a mark is registered. The (R) symbol must not be used unless registration is confirmed for the applicable jurisdiction and goods or services.

2. Permitted and prohibited use

Customers may use ordinary product outputs and reports for their internal operations and authorized business communications during the subscription. They may not extract or reuse platform branding, templates, or interface elements to create a competing product; remove notices; imply endorsement; register confusing domains or marks; or publish confidential product materials without written permission.

Any public logo, media, reseller, co-branding, or investor use requires the current brand guidelines and written approval.

3. Customer and third-party materials

Customers retain ownership of Customer Data and must have permission to use third-party logos, documents, photos, insurer materials, and other content they upload. References to third-party products remain the property of their owners and do not imply endorsement.

Copyright or trademark concerns may be sent to legal@restorecheckiq.ca with identification of the work or mark, location, authority, contact information, and requested action.



Customer Support & Service Commitment

How support is requested, classified, accessed, measured, and kept separate from customer work.

Effective July 24, 2026	Version 2026.07.24	Audience Customers, authorized users, and support contacts
----------------------------	-----------------------	---

1. Support scope and routing

RestoreCheck IQ provides a separate support workspace for platform, usage, account, integration, billing, privacy, and security issues. Cases may be automatically classified and routed using the subject and description, but support staff can correct the classification.

Support performance may be measured using privacy-minimized case metadata. Customer project and document content is excluded from routine support dashboards.

2. Safe diagnostic access

- Support personnel receive separate platform roles and only the diagnostic categories needed for assigned work.
- Access requires a case, purpose, and auditable record; private notes and customer project content are not routine support data.
- Exceptional access to customer content requires explicit authorization, minimum scope, time limit, and oversight.
- Support personnel cannot grant themselves platform-owner authority, access investor exports, change customer ownership policy, or bypass tenant scope.
- Never send a password, authenticator seed, recovery code, full API key, or unnecessary evidence through a support description.

3. Priority and communications

Security threats, widespread unavailability, and data-integrity risk receive priority over general questions and feature requests. Response and resolution targets shown in the platform are operational objectives unless a signed service-level agreement makes them binding.

Request support in the application or at support@restorecheckiq.ca. Report active security incidents to security@restorecheckiq.ca.



Subscription, Billing & Cancellation Policy

The controlled signup, payment confirmation, activation, renewal, cancellation, and refund process.

Effective July 24, 2026	Version 2026.07.24	Audience Applicants, customers, billing contacts, and administrators
----------------------------	-----------------------	---

1. Registration and activation

A signup submission is an application only. It does not create an organization, user, password, or session. RestoreCheck IQ reviews the organization and selected subscription, confirms the applicable payment state, and then issues a single-use activation link.

The activation user creates a permanent password and completes required two-factor authentication. RestoreCheck IQ does not email reusable temporary passwords.

2. Plans, payment, and taxes

Plan features, seat or usage limits, billing cycle, fees, currency, payment method, renewal, and special commitments appear in the order or subscription confirmation. Customers authorize charges or agree to pay invoices according to that document and are responsible for applicable taxes.

A preference selected during application is not a final price or acceptance. Card information is handled by the configured payment provider when card billing is enabled.

3. Renewal, cancellation, and refunds

Renewal and notice periods are governed by the applicable order. A cancellation stops future renewal but does not ordinarily refund an already-started paid period or erase outstanding charges, except where the order or law requires otherwise.

Before closure, an authorized administrator should request an available export. Workspace closure uses a documented retention and recoverability process; legal holds, tax records, security evidence, and backup rotation may delay complete deletion.

Billing questions and cancellation requests may be submitted through the authenticated support centre or to support@restorecheckiq.ca.



POLICY 15 / DELETE AN ACCOUNT

Account & Data Deletion Request

A public route for requesting deletion, including the verification and retention process.

Effective July 24, 2026	Version 2026.07.24	Audience Current and former applicants, users, and customer administrators
----------------------------	-----------------------	---

1. How to request deletion

Email privacy@restorecheckiq.ca from the address associated with the account with the subject "Account deletion request". Identify the organization and whether you are requesting deletion of your individual user account, a registration application, or an entire customer workspace. Do not send a password, authenticator seed, API key, or unnecessary customer evidence.

Current users may also open an authenticated privacy support case. An individual user cannot delete an organization or records the organization is legally entitled to control; workspace closure requires verified administrator authority.

2. Verification and effect

We verify identity and authority using account, organization, and security records. We may contact the customer organization where it controls the data. Once approved, access is revoked and eligible personal information and customer data are deleted or de-identified through the documented lifecycle.

Some information may be retained where reasonably necessary for law, taxes, security, fraud prevention, disputes, legal holds, or backup rotation. We will explain material retention that applies to the request. Deletion does not require RestoreCheck IQ to remove de-identified information that can no longer reasonably identify a person.

3. Timing and confirmation

We will acknowledge the request, request any needed verification, and provide a status or outcome within the period required by applicable law. Complex requests, legal restrictions, or customer-controlled records may require additional time, which we will explain.

Questions or complaints about the process may be directed to the Privacy Officer at privacy@restorecheckiq.ca.