



Richweb 2026 Privacy Policy

Last Updated: 12-31-2025[Month Day, Year]

Richweb, Inc. is committed to protecting the confidentiality and security of documents and other content that our business customers submit to us.

This Document Privacy Policy explains how we handle Customer Documents in connection with our managed IT services, network engineering projects, and cloud services and hosting (collectively, the "Services"). Our practices are designed to align with the SOC 2 Trust Services Criteria for Security, Availability, and Confidentiality.

1. Scope and Relationship to Other Policies

This policy applies specifically to Customer Documents and their associated metadata processed through our Services.

Other information we collect—such as contact information, billing details, and website usage data—is governed by our general Privacy Policy included in the Richweb Information Security Policy.

If there is any conflict between this Document Privacy Policy and our general Privacy Policy regarding Customer Documents, this policy will govern.

2. Key Definitions

Customer: A business or organization that has a contractual agreement with Richweb to receive the Services.

Customer Documents: Any files, documents, configurations, backups, logs, text, images, or other data that you or your authorized users provide to us or that we handle on your behalf in connection with the Services.

Authorized Users: Individuals that the Customer permits to interact with Richweb systems or Services on its behalf (e.g., employees, contractors, or other representatives).

As the Customer, you are responsible for ensuring that Customer Documents you provide or authorize us to access comply with your legal, regulatory, and contractual obligations.



4. How We Use Customer Documents

We use Customer Documents only as necessary to:

1. Deliver and support the Services

- Operate, maintain, and support your IT infrastructure, networks, systems, and hosted environments

- Perform network engineering projects, configuration changes, and troubleshooting

- Provide backups, restores, migrations, and related managed services

2. Secure and improve the Services

- Monitor systems and networks for performance, availability, and security

- Detect, prevent, and respond to security threats, incidents, and misuse

- Improve reliability and service quality, consistent with your agreements with us

3. Meet legal and contractual obligations

- Comply with applicable laws, regulations, and lawful requests

- Enforce our contracts, including Master Service Agreements, Statements of Work, and related terms

We do not:

- Sell Customer Documents

- Use Customer Documents for advertising

- Use Customer Documents to train public or shared AI models

5. Access to Customer Documents

Access to Customer Documents is limited and controlled:

- Our systems and tools are designed so Customer Documents are accessed by personnel only when needed to deliver or support the Services.



- Only authorized Richweb personnel with a legitimate business need (e.g., support engineers, network engineers, operations, security) may access Customer Documents.
- We apply role-based access control (RBAC) and the principle of least privilege; access is reviewed and adjusted as roles change.
- Access for support or project work is typically initiated by your request (e.g., tickets, change orders) and is limited to the scope necessary to perform that work.
- Access to environments and data is logged and monitored where technically feasible, and is subject to internal policies and oversight.

6. Data Storage, Encryption, and Security

We employ administrative, technical, and physical safeguards designed to protect Customer Documents in line with SOC 2-aligned practices, including:

- Encryption
 - Encryption in transit using industry-standard protocols (e.g., TLS) where supported.
 - Encryption at rest for hosted data and backups, using industry-standard algorithms where supported by the underlying infrastructure.
- Access Controls & Authentication
 - Role-based access and least-privilege authorization for production systems.
 - Strong authentication for internal systems, including multi-factor authentication (MFA) where applicable.
 - Strict handling and protection of administrative and privileged credentials.
- Infrastructure & Network Security
 - Use of firewalls, segmentation, and security tooling appropriate to the environment.
 - Regular patching and maintenance of systems and supported platforms.
 - Secure configuration baselines and change control processes for managed infrastructure.
 - Monitoring for unusual or suspicious activity.
 - Periodic internal reviews and security assessments.



- Personnel and Process Controls

- Confidentiality obligations for employees and contractors with access to Customer Documents.
- Security and privacy training for relevant personnel.
- Documented policies and procedures governing handling of customer environments and data.

While no system can be guaranteed 100% secure, we continuously work to maintain and enhance our security posture.

7. Data Retention and Deletion

- We retain Customer Documents for the duration of your engagement with Richweb and as reasonably necessary to provide the Services, meet legal obligations, and enforce our agreements.
- Specific retention periods (for example, for backups, logs, or archives) may be defined in your contract, Statement of Work, or service configuration.
- Upon your instruction—subject to technical feasibility and applicable law—we will delete or return specific Customer Documents within a commercially reasonable timeframe.
- When Customer Documents are deleted, they are removed from active systems and subsequently purged from backups based on our standard backup and retention schedules.

Customers seeking detailed retention information for their specific environment should refer to their contract or contact us at [Privacy/Support Email].

8. Your Responsibilities

As a B2B Customer, you are responsible for:

- Ensuring you have the rights and legal basis to provide access to Customer Documents and systems that we manage or host on your behalf.
- Providing appropriate privacy notices and obtaining consents, where required, for individuals whose data may be contained in Customer Documents or systems we support.
- Configuring user access, permissions, and authentication for your own users (including MFA for your accounts where available) and notifying us of changes in authorized contacts.



- Avoiding use of the Services in a way that violates applicable laws or your contracts, including restrictions on certain regulated data types where not expressly agreed in writing.

We are available to discuss best practices for securely using our Services in your specific environment.

9. Incident Response and Security Events

We maintain an incident response program designed to promptly address security events affecting Customer Documents or environments we manage:

- We investigate suspected incidents, take steps to contain and remediate them, and work to prevent recurrence.
- For confirmed incidents that materially affect the confidentiality, integrity, or availability of Customer Documents or managed systems, we will notify affected Customers without undue delay, consistent with applicable law and our contractual obligations.
- We will provide relevant information reasonably necessary to support your own investigations, notifications, or regulatory obligations, to the extent permitted by law and subject to confidentiality constraints.

10. Changes to This Document Privacy Policy

We may update this Document Privacy Policy from time to time to reflect changes in our Services, technologies, or legal requirements.

- When we make material changes, we will update the "Last Updated" date at the top of this page.
- Where appropriate, we may provide additional notice (for example, via email to customer contacts or through your account portal).

Your continued use of the Services after changes become effective constitutes your acceptance of the updated policy.

11. Contact Us

Richweb, Inc.

www.richweb.com

Email: Info@richweb.com

(804) 369-0421