Clear Cyber Advisory Privacy Policy

Last updated: June 23, 2026

Clear Cyber Advisory (“Clear Cyber Advisory,” “we,” “us,” or “our”) respects privacy, confidentiality, and responsible information handling. This Privacy Policy explains how we collect, use, disclose, retain, and protect information when you visit our website, contact us, download a resource, submit a form, request a consultation, or work with us.

Clear Cyber Advisory provides cybersecurity and technology advisory services, including cyber insurance readiness, Shadow AI risk discovery, AI use policy support, and secure AI workflow automation advisory. Because these services may involve sensitive business, technical, operational, or security-related information, we apply practical safeguards and expect clients to share only the information reasonably necessary for the engagement.

This Privacy Policy is intended to apply to website visitors, prospective clients, clients, business contacts, and other individuals who interact with us from Canada, the United States, and other locations.

1. Who We Are

Clear Cyber Advisory is a cybersecurity advisory business focused on helping small and medium-sized organizations improve cyber readiness, reduce Shadow AI risk, and approach secure AI workflow automation with clarity and practical controls.

For privacy questions or requests, see contact in Section 25.

2. Scope of This Policy

This Privacy Policy applies to information we collect through:

* Our website
* Contact forms
* Email communications
* Consultation requests
* Resource downloads

* Client intake forms
* Advisory engagements
* Proposals, reports, and related business communications

This Privacy Policy does not apply to third-party websites, platforms, tools, or services that we do not control, even if our website links to them.

A separate client agreement, statement of work, confidentiality agreement, or data-processing agreement may apply to specific client engagements. If there is a conflict between this Privacy Policy and a signed client agreement, the signed client agreement will generally govern that engagement.

3. Types of Information We Collect

We may collect personal information, business information, technical information, and confidential client information depending on how you interact with us.

Information you voluntarily provide

You may provide information such as:

* Name
* Business name
* Job title
* Email address
* Phone number, if you choose to provide it
* Website address
* Industry or business type
* Message content
* Consultation request details
* Information submitted through forms, email, documents, or other communications
* Billing, payment, tax, and business administration information, where applicable

Business and advisory information

During advisory work, we may receive or review information about your organization, such as:

* Cyber insurance questionnaires, applications, renewal questions, or evidence requests
* Security policies, procedures, and checklists
* IT, cloud, email, identity, access, endpoint, backup, and vendor information
* Business workflows, approval steps, automation ideas, and data flows
* AI tools used by staff, contractors, departments, or vendors
* Shadow AI risks, data exposure concerns, or AI governance gaps
* Internal documentation, screenshots, forms, diagrams, or reports you choose to share
* Business risks, control gaps, recommended improvements, and implementation priorities

Technical website information

When you visit our website, we may automatically collect limited technical information, such as:

* IP address
* Browser type and version
* Device type
* Operating system
* Pages visited
* Date and time of visit
* Referring website
* Approximate location based on browser, device, or IP information
* Basic analytics, performance, and security logs

We do not knowingly collect personal information from children, and our website and services are not directed to children.

4. Information We Do Not Want You to Send Casually

Unless we have agreed on a secure process in advance, please do not send us:

* Passwords
* Private keys
* Recovery phrases
* Full credential lists
* Unmasked access tokens

* Sensitive personal health information
* Payment card numbers
* Government identity documents
* Highly sensitive regulated data
* Confidential client files that are not necessary for the advisory work
* Production system access unless specifically agreed in writing

For most advisory work, we can provide useful guidance from descriptions, screenshots, questionnaires, policies, workflow summaries, and limited evidence without needing direct system access or sensitive secrets.

If sensitive information must be shared, we should first agree on an appropriate secure method.

5. How We Use Information

We may use information for the following purposes:

* To respond to inquiries
* To provide requested resources
* To schedule consultations
* To understand your business needs
* To prepare proposals, scopes of work, reports, summaries, checklists, and action plans
* To provide cyber insurance readiness advisory services
* To provide Shadow AI risk discovery and AI use policy support
* To provide secure AI workflow automation advisory services
* To communicate with you about services, questions, risks, recommendations, and next steps
* To manage client relationships
* To maintain business, tax, accounting, billing, and administrative records
* To operate, maintain, secure, and improve our website and business systems
* To detect, prevent, or respond to misuse, fraud, security incidents, or unauthorized activity
* To comply with legal, regulatory, contractual, insurance, accounting, or professional obligations
* To protect our rights, clients, systems, business operations, and reputation

We may also use aggregated or de-identified information to improve our services, develop internal templates, identify common risk patterns, or create educational materials. We do not intentionally identify a client in public materials without permission.

6. Client Confidentiality and Advisory Materials

We treat client information shared during advisory work as confidential business information, whether or not it is personal information.

This may include:

* Intake responses
* Cyber insurance readiness information
* Shadow AI findings
* AI tool inventories
* Workflow maps
* Security-control notes
* Reports, recommendations, and action plans
* Client documents, screenshots, and communications

We do not disclose client confidential information except where:

* The client authorizes the disclosure
* Disclosure is necessary to provide the requested services
* Disclosure is required by law, regulation, court order, or lawful process
* Disclosure is necessary to protect rights, safety, security, or business operations
* Disclosure is permitted under a signed client agreement

A separate client agreement, statement of work, or confidentiality agreement may include additional confidentiality terms.

7. Use of AI Tools

Because our work may involve AI risk and secure workflow automation, we may discuss or evaluate AI tools, automation tools, and related business processes.

We do not intentionally submit client confidential information, passwords, private keys, regulated data, or highly sensitive business information into public AI tools unless the client has approved the process and appropriate safeguards have been considered.

Where AI tools are used to support internal drafting, summarization, organization, or analysis, we aim to minimize unnecessary disclosure of personal, confidential, or security-sensitive information.

Clients remain responsible for deciding what information they provide to us and for approving any AI-related tool, workflow, vendor, policy, or automation used in their own business.

8. Legal Basis for Processing

Depending on where you are located and the nature of the information, we may rely on one or more legal bases to collect and use information, including:

* Your consent
* The need to respond to your request
* The need to prepare, perform, or manage a contract
* Our legitimate business interests
* Compliance with legal, regulatory, tax, accounting, or contractual obligations
* Protection of rights, security, safety, or business operations

Where we rely on consent, you may withdraw consent where legally available. Withdrawal of consent may affect our ability to provide certain services.

9. Email Communications and Marketing

If you contact us, request information, download a resource, subscribe to updates, or otherwise consent to receive communications, we may send you service-related messages, cybersecurity resources, business updates, or marketing communications.

Marketing communications may include information about cyber insurance readiness, Shadow AI risk, AI workflow automation, cybersecurity readiness, or Clear Cyber Advisory services.

You may unsubscribe from marketing communications at any time by using the unsubscribe option where provided or by contacting us directly; see contact in **Section 25.**

We aim to comply with Canada's Anti-Spam Legislation, U.S. commercial email rules, and other applicable communication laws.

Even if you unsubscribe from marketing communications, we may still send service-related or transactional messages, such as replies to your inquiry, meeting details, proposal communications, project updates, invoices, contract notices, or legally required communications.

10. Cookies, Analytics, and Similar Technologies

Our website may use cookies, pixels, log files, analytics tools, and similar technologies to support website functionality, understand website traffic, improve user experience, measure performance, and maintain security.

Cookies are small files stored on your device. You can control, block, or delete cookies through your browser settings. Some website features may not function properly if cookies are disabled.

We may use third-party website, analytics, or performance tools that collect limited technical information such as browser type, device type, pages visited, time on page, referring website, and approximate location.

We do not use cookies to knowingly collect passwords, private keys, or highly sensitive personal information.

At this time, our website is intended to be simple and informational. If we later add more advanced tracking, advertising pixels, remarketing, or consent-management tools, we may update this Privacy Policy.

11. Third-Party Service Providers

We may use trusted third-party service providers to operate our website, communicate with clients, store documents, process payments, manage scheduling, and support business operations.

These providers may include:

* Website hosting and design platforms
* Domain, DNS, and email service providers
* Analytics and website performance tools
* Contact form providers
* Scheduling tools
* Cloud storage and document management tools
* Email and communication tools
* Payment processors
* Accounting, bookkeeping, and tax tools
* Professional advisors
* Security, backup, and administrative tools

These providers may access or process information only as needed to provide services to us, support our business operations, comply with law, or fulfill their own legal obligations.

We do not sell personal information.

We do not share client confidential information with third parties for their independent marketing purposes.

12. International Processing and Cross-Border Transfers

Clear Cyber Advisory may serve clients and website visitors located in Canada, the United States, and other countries.

Information may be collected, processed, stored, or accessed in Canada, the United States, or other countries where we or our service providers operate. Privacy laws in those locations may differ from the laws in your province, state, or country.

By interacting with us or using our website, you understand that information may be processed outside your location, subject to applicable law and reasonable safeguards.

Where required, we aim to use appropriate contractual, organizational, and technical measures to protect information involved in cross-border processing.

13. Security Safeguards

We use reasonable administrative, technical, and organizational safeguards designed to protect information against unauthorized access, loss, misuse, disclosure, alteration, or destruction.

Safeguards may include practical measures such as access control, account security, secure storage practices, limited sharing, vendor selection, and reasonable internal handling procedures.

However, no website, email system, cloud platform, network, or method of electronic transmission is completely secure. We cannot guarantee absolute security.

If we become aware of a security incident involving personal information or client confidential information, we will assess the situation and take reasonable steps based on the nature of the incident, the information involved, applicable law, and any contractual obligations.

14. Retention of Information

We retain information only as long as reasonably necessary for the purposes described in this Privacy Policy, including:

* Responding to inquiries
* Providing services
* Maintaining client and business records
* Meeting legal, tax, accounting, insurance, and contractual requirements
* Resolving disputes
* Enforcing agreements
* Protecting rights, security, and business operations

Retention periods may vary depending on the type of information, the nature of the relationship, legal requirements, and business needs.

When information is no longer reasonably required, we may delete, anonymize, archive, or securely retain it according to our legal and business requirements.

15. Your Privacy Rights and Choices

Depending on where you live, you may have rights regarding your personal information. These rights may include the right to:

* Request access to personal information we hold about you
* Request correction of inaccurate or incomplete information
* Request deletion of personal information, where legally available
* Withdraw consent, where processing is based on consent
* Object to or restrict certain processing, where legally available
* Request information about how we collect, use, disclose, or retain personal information
* Request a copy of certain personal information, where legally available
* Opt out of marketing communications

These rights are not absolute and may be subject to legal, contractual, security, identity-verification, privilege, confidentiality, and record-keeping requirements. To make a privacy request, use the contact information provided in Section 25**.** We may need to verify your identity before responding.

16. Canada Privacy Notice

For individuals in Canada, we aim to handle personal information in accordance with applicable Canadian private-sector privacy laws, including principles of accountability, identifying purposes, consent, limiting collection, limiting use and disclosure, safeguards, openness, individual access, and appropriate correction.

You may contact us to ask questions, request access to your personal information, request correction, withdraw consent where applicable, or raise a privacy concern.

If you are not satisfied with our response, you may have the right to contact the appropriate privacy regulator in your jurisdiction.

17. United States and California Privacy Notice

If you are located in the United States, including California or another state with applicable privacy laws, you may have additional rights depending on the law that applies to you and to us.

Subject to applicable thresholds, exemptions, and legal requirements, these rights may include the right to know, access, correct, delete, or receive information about certain uses or disclosures of personal information.

We do not sell personal information.

We do not knowingly share personal information for cross-context behavioral advertising as that term is commonly used under California privacy law.

We do not knowingly collect, sell, or share personal information of children.

We do not discriminate against individuals for exercising privacy rights.

Because U.S. state privacy laws vary and may apply differently depending on business size, data use, revenue, residency, and other factors, some rights may not apply in every situation.

18. European Economic Area, United Kingdom, and Other International Visitors

If you are located in the European Economic Area, the United Kingdom, Switzerland, or another jurisdiction with similar privacy laws, you may have additional rights depending on applicable law.

These rights may include:

* Access to your personal information
* Correction of inaccurate information
* Deletion of personal information
* Restriction of processing
* Objection to processing
* Data portability
* Withdrawal of consent where processing is based on consent

* The right to lodge a complaint with a privacy or data protection authority

We may process information based on consent, contract, legitimate interests, legal obligations, or other lawful bases recognized by applicable law.

Clear Cyber Advisory is a small advisory business based outside the European Union and does not intentionally target individuals in the European Economic Area with consumer services. However, if we interact with an international business contact, prospective client, or client, we aim to handle personal information in a reasonable and privacy-conscious manner.

19. Business Contacts and Client Representatives

Many individuals who interact with us do so in a professional or business capacity. This may include business owners, executives, employees, contractors, consultants, insurance brokers, IT providers, legal advisors, accounting professionals, or other client representatives.

We may use business contact information to communicate about services, projects, proposals, meetings, reports, renewals, invoices, cybersecurity resources, or related business matters.

Where required by law, you may request access, correction, deletion, unsubscribe, or other available privacy rights using the contact information provided in Section 25.

20. Payment and Billing Information

If payment is required for services, we may use third-party payment processors, banks, accounting tools, or bookkeeping systems to process and record payments.

We do not intentionally collect or store full payment card numbers on our website unless this is handled by a payment processor or platform designed for that purpose.

Billing and transaction records may be retained as required for tax, accounting, legal, audit, and business purposes.

21. Links to Other Websites

Our website may contain links to third-party websites, documents, platforms, tools, or resources. We are not responsible for the privacy practices, security, content, or policies of third-party websites or services.

You should review the privacy policies and terms of any third-party websites or services you choose to use.

22. Public Resources and Downloadable Materials

We may provide guides, checklists, articles, templates, or other resources for educational and informational purposes.

If you submit your email address or other information to receive a resource, we may use that information to deliver the resource, respond to related requests, and communicate with you as described in this Privacy Policy.

Resources are not intended to require you to submit passwords, private keys, credentials, regulated data, or highly sensitive information.

23. No Sale of Personal Information

We do not sell personal information. We do not rent client lists.

We do not disclose client confidential information to third parties for their independent marketing purposes.

If our practices change in the future, we will update this Privacy Policy and provide choices where required by law.

24. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our services, website, legal requirements, tools, vendors, or business practices.

The updated version will be posted on our website with a revised “Last updated” date.

If we make material changes, we may provide additional notice where appropriate.

Your continued use of our website or services after an updated Privacy Policy is posted means that the updated version applies going forward, subject to applicable law and any signed client agreement.

25. Contact Us

If you have questions about this Privacy Policy, want to make a privacy request, want to unsubscribe from marketing communications, or want to raise a privacy concern, please contact us:

Clear Cyber Advisory

Email: martin@clearcyberadvisory.com

Website: https://www.clearcyberadvisory.com