MINICYBER

Terms of Service & Master Services Agreement

Business Name: MINICYBER
ABN: 19 541 815 072
Website: minicyber.com.au
Jurisdiction: Western Australia

> **Important Notice:** By accepting a Quote, Statement of Work (SOW), or paying an invoice issued by MiniCyber, you acknowledge that you have read, understood, and agreed to be bound by these Terms of Service.

1. Agreement Structure

This Terms of Service document operates as a Master Services Agreement (MSA) governing the overarching legal and operational relationship between MiniCyber ("the Provider", "we", "us") and the client ("the Client", "you").

The specific technical deliverables, services, and pricing (such as the *Mini-Biz Security Baseline*, *Peace of Mind* package, or bespoke Incident Response) will be defined in a separate Quote or Statement of Work (SOW). This modular approach ensures that specific project details can change without requiring renegotiation of these foundational legal terms.

2. Provision of Services

MiniCyber provides specialised cyber security consulting, remote support, and implementation services tailored for individuals, sole traders, and small businesses.

- **Reasonable Care and Skill:** We will deliver all services with due care and skill, aligning with general industry best practices for small business IT security.
- **Remote Support:** Services are predominantly delivered remotely using secure third-party remote access tools. On-site visits incur an additional call-out fee as detailed in our pricing structure.
- **Incident Response (Break-Fix):** Clients engaging us for emergency incident response without an ongoing managed agreement will be billed at our emergency hourly rates and receive support on a "best-effort" basis.

3. Shared Responsibility & Cybersecurity Realities

Cyber security is an ongoing process of risk mitigation, not an absolute guarantee. You acknowledge that no combination of hardware, software, or services can provide 100% protection against all cyber threats, zero-day exploits, or determined malicious actors. Furthermore, even when all recommended security controls are implemented, no system is entirely immune to compromise. MiniCyber is not liable for any breach, data loss, or system compromise that successfully bypasses these security measures.

- **Risk Acceptance Waiver:** Our service effectiveness relies on a "Shared Responsibility Model". If we formally recommend a critical security control (such as Multi-Factor Authentication, patching, or specific endpoint protection) and you decline to implement it due to budget, convenience, or other reasons, MiniCyber accepts zero liability for any subsequent breach, data loss, or system compromise resulting from that unmitigated vulnerability.
- **Human Error & Financial Fraud:** While we implement technical controls to reduce risk, cyber security ultimately relies on human vigilance. MiniCyber is not liable for any financial losses, misdirected funds, or invoice fraud (such as Business Email Compromise) resulting from a client or their staff being deceived by social engineering, phishing, or spoofed communications.
- **Ransomware & Data Recovery:** In the event of a ransomware attack, MiniCyber will assist with incident containment (billed at emergency rates unless otherwise contracted). However, MiniCyber accepts no liability for your decision to pay or not pay criminal extortion demands. Furthermore, we are not a specialised data recovery or digital forensics firm; we do not guarantee the recovery, decryption, or restoration of lost or encrypted data.

- **Awareness Training & Simulations:** Any staff awareness briefings or phishing simulations provided by MiniCyber are for educational purposes only. We do not guarantee that participating staff will successfully identify or prevent future cyber attacks.
- **Client Cooperation:** The Client must provide timely access to systems, administrative credentials, and accurate information required to perform the services. Delays caused by the Client may result in paused services.

4. Third-Party Inputs & Subscriptions

Modern IT delivery relies heavily on third-party software, cloud infrastructure, and service providers (e.g., Endpoint Protection platforms, email hosts, password managers).

- **Liability for Third-Party Failures:** MiniCyber configures and manages these tools but is not the software developer or hosting provider. We are not liable for outages, permanent data loss, or security breaches originating from a third-party vendor's infrastructure or native software flaws. Your use of these products is subject to the respective vendor's End User License Agreement (EULA).
- **Licensing Costs:** Unless explicitly stated in your SOW, the costs for third-party software licences are billed separately and paid directly by you or via our designated procurement partners.

5. Limitation of Liability

This section is critical and dictates the allocation of risk in our commercial relationship, drafted in accordance with Australian law.

5.1 Australian Consumer Law (ACL)

Nothing in these terms excludes, restricts, or modifies any consumer guarantee, right, or remedy conferred by the Australian Consumer Law (Schedule 2 of the *Competition and Consumer Act 2010* (Cth)) that cannot be lawfully excluded. For services not ordinarily acquired for personal, domestic, or household use, our liability for failure to comply with a consumer guarantee is limited, at our discretion, to:

- Supplying the services again; or
- Paying the cost of having the services supplied again.

5.2 Financial Cap & Unfair Contract Terms (UCT)

To ensure a fair and proportionate allocation of risk for a small business engagement, and in compliance with the Australian Unfair Contract Terms (UCT) regime, both parties agree to a mutual liability cap. The total aggregate liability of MiniCyber for any claim arising out of or in connection with these services—whether in contract, tort (including negligence), or otherwise—shall not exceed the total fees paid by the Client to MiniCyber in the twelve (12) months immediately preceding the event giving rise to the claim.

5.3 Exclusion of Consequential Loss

To the maximum extent permitted by law, MiniCyber shall not be liable for any indirect, incidental, special, or consequential losses, including but not limited to:

- Loss of profits, revenue, or anticipated savings;
- Loss of business opportunity or goodwill;
- Permanent loss, corruption, or destruction of digital data;
- Fines or regulatory penalties incurred by the Client.

6. Confidentiality and Privacy

As a small business (under $3 million annual turnover), MiniCyber generally falls under the small business exemption of the *Privacy Act 1988* (Cth). However, given the sensitive nature of cyber security, we voluntarily commit to strict confidentiality:

- We will only use your data and credentials for the express purpose of delivering the agreed services.

- We will never sell your information to third parties.
- Upon termination of services, any administrative credentials held by MiniCyber will be securely handed over and destroyed from our systems.

7. Fees, Invoicing & Payment

- **Invoicing:** Invoices are generated and managed via our accounting partner (Hnry).
- **Payment Terms:** Payment is strictly due within the timeframe specified on the invoice (typically 7 or 14 days).
- **Suspension of Service:** MiniCyber reserves the right to suspend ongoing services or refuse emergency support if client payments fall into arrears.

8. Term & Termination

For ad-hoc or project-based work (e.g., audits, baseline implementations), the agreement terminates upon project completion and final payment. For any ongoing monthly services (if applicable), either party may terminate the agreement for convenience by providing thirty (30) days written notice. Early termination fees do not apply, but you remain liable for any services rendered up to the date of termination.

9. Governing Law

This Agreement is governed by the laws of Western Australia. The parties irrevocably submit to the exclusive jurisdiction of the courts of Western Australia.