This is your Waratah Cyber Insurance Policy. We want to make sure you know what you’re getting for your premium, so we made this policy clear and concise. Please take a few minutes to read it carefully and let us know if you have questions. We are happy to work with you to change or amend coverage.

**Who’s covered?**

This policy covers **(INSERT INSURED)** its subsidiaries and its employees (including contracted temporary employees). For convenience, this policy refers to the covered companies as “your business” and those covered companies and persons as “You.” You can add more insureds, as long as we agree in writing they are insured.

**When?**

This policy only covers claims made and notified to us from the events described below that start after (**INCEPTION DATE)** and **(TIME)** and before 12 months after **(INCEPTION DATE)** and **(TIME)** (which this policy calls the “policy year”). You need to notify us of any events as soon as possible and in writing, and before the end of the policy year. If you don’t do this, you aren’t covered.

**Against what events?**

We protect your business against ***monetary loss*** caused by one of these three events during the year:

* a cyberattack against your business or its website by malicious external or inside parties, including malware, phishing, or ransomware,
* your loss of a laptop or mobile phone that causes your business accidentally to lose its data or the personal information of your business’ customers or employees, or
* a cyberattack against your business’ cloud provider by malicious external parties that causes the cloud provider accidentally to lose your business’ data or the personal information of your business’ customers or employees.

***Monetary loss*** can include loss caused by a shutdown of your business’ computer network, a ransom demand, or funds your business loses due to a fraudulent funds transfer, all because of a cyberattack to your business. We also cover you for loss or damage that others may accuse you of causing because of a cyberattack on your business. There are important limitations, so please read on.

**What is a cyberattack?**

A cyberattack is any targeted malicious or deliberate exploitation of:

* any security measures protecting, or
* any software, firmware, or hardware component of,

your business’ or your cloud provider’s computers, computer systems or networks, or any interrelated computing devices, mechanical or digital machines connected to your business or its operations, to damage, disrupt, deny access to, or use of, or gain unauthorized access to or use of any components or data they store or transmit.

**For how much?**

We provide your business with insurance for your ***monetary loss*** up to the coverage limits indicated in the Policy Schedule for the year. Each coverage limit is the maximum we will reimburse you in total for that coverage, up to the Aggregate Limit for all policy coverages indicated in the Schedule for the year - even if your losses are larger.

**And now, more detail…**

1. **If your business or its website suffers a cyberattack during the year, including a ransomware or denial of service attack, we cover:**

* **Profits your business loses as a direct result of the cyberattack, if the cyberattack prevents your business from operating,**
* **Damage to or loss of your business’ physical property caused directly by the cyberattack,**
* **Bodily injury or personal injury to your business’ customers or employees caused directly by the cyberattack, and**
* **Theft of, damage to, or loss of your business’ data, your customers’ or employees’ personal information caused directly by the cyberattack.**

If such a cyberattack occurs, we include cover for the computer emergency response costs we incur with the help of our team of experts to restore your business’ computer network to its operations just before the cyberattack and remedy the cause of any data breach your business suffered to ensure it is contained. We won’t cover any costs you incur to upgrade your hardware, software or other systems. That’s because we’re only covering the emergency costs of restoring your network to its operations, not an IT overhaul.

We only cover lost profits directly resulting from a cyberattack preventing your business from operating for up to 15 days after the cyberattack or until your business is restored to its operations just before the cyberattack, whichever is first. Of course, we don’t have to pay to put your business in a better position than if there were no cyberattack.

If a cyberattack on your business, a lost laptop or mobile phone, or a cyberattack on your business’ cloud provider by external malicious parties during the policy year causes the loss of your business’ data, your business’ customers’ or employees’ personal information, contact us and our incident response partners will investigate the cyberattack on your business to ensure the problem is contained as soon as possible and that those individuals and regulators are notified to the extent required by law. We’ll cover your business for those costs, but only if we incur them.

We will deal with coverage for theft of your business’ funds through a phishing attack a little later.

**What’s not included in this coverage:**

We don’t cover loss or damage to intangible things like your business’ valuation, intellectual property, reputation, or credit rating. Lost wages and non-cash financial instruments (like shares or cryptocurrency) also aren’t covered.

Of course, we don’t cover your business’ cloud provider for its own costs or losses from a cyberattack on it.

1. **If your business suffers a phishing attack during the policy year and your employee unintentionally falls victim to it by opening an email or clicking an attachment they shouldn’t, thereby allowing a hacker to access your business’ computer network to fraudulently direct a funds transfer of your business’ funds to an external account, then we will reimburse your business for that theft of your business’ funds.**

**We will also reimburse your business for a fraudulent funds transfer if a hacker impersonates your business’ website and/or domain name for the purposes of directing your business’ funds to a fraudulent account.**

**What’s not included in this coverage:**

Bitcoins or other cryptocurrency and other non-bank financial instruments such as cash, invoices, shares and debt instruments are not covered. We want to help you protect your business against phishing attacks it might be exposed to, but not for other types of crime which should be covered under your other insurance.

We don’t cover theft of your business’ funds if your employee is involved in arranging a fraudulent wire transfer beyond simply falling victim to a phishing attack by opening an email or clicking on an attachment they shouldn’t.

1. **If a cyberattack directly on your business during the year accidentally causes your business to damage or injure others or their property or data, we will protect you if someone makes a complaint or files a claim that you caused them to suffer a privacy breach, bodily injury, or property damage due to that cyberattack against your business.**

If needed, we’ll provide legal defense at our own expense and pay the damages on your behalf. As we have already mentioned, the maximum amount we’ll pay in damages in total for the year is indicated in the Schedule.

Since we’re paying for the defense, we may investigate, settle, or contest the complaint as we judge best.

**What’s not included in this coverage:**

We do not cover third party claims of stress, mental anguish unless arising directly from a cyberattack against your business. We do not cover reputational damage.

Damage caused by drones, other flying machines, or motorised vehicles of any kind (such as electric bikes, segways, or electric skateboards) aren’t covered.

1. **If your business or its website suffers a cyberattack during the year, including a malware, ransomware, denial of service or phishing attack, that causes it to lose your customers’ personal information, we will cover any fines, penalties, or costs that a regulator or payment card brand demands in writing that you pay them.**

If your business handles payment card transactions, your business may be liable to its payment card brands if they demand in writing, asserting that your business breached their Payment Card Industry compliance standards when a cyberattack on your business caused the loss of your customers’ or your employees’ personal information. Or a regulator may investigate whether your business violated a regulation regarding a cyberattack on your business that caused your business to lose its customers’ personal information.

If needed, we’ll cover your legal costs for defending a demand and/or responding to a regulatory investigation arising from a cyberattack and pay on your behalf any fines, penalties or costs assessed, but the maximum amount we’ll pay in fines, penalties and costs in total for the year is indicated in the Schedule. Again, since we’re paying for the defense, we may investigate, settle, or contest the action as we judge best.

**What’s not included in this coverage:**

We can only pay those fines and penalties that we are allowed to by law.

**Other things not covered under this policy:**

This policy covers your business only for loss or damage caused by a cyberattack on your business, such as hacking, malware attacks, phishing, ransomware, or denial of service attacks, a cyberattack on your business’ cloud provider, or loss of your business’s laptop or mobile phone. Everything else unrelated to a cyberattack or lost laptop or mobile phone, such as a “power failure,” “a glitch,” “I forgot to renew my software licence”, a plain old “equipment or software failure”, “programming error”, or insolvency isn’t covered.

We do not cover intentional damage by you, nor losses that should ordinarily have been foreseen or prevented by you through reasonable steps.

We don’t cover loss or damage caused intentionally, or as a result of illegal activity, by you.

We don’t cover damages or matters usually covered by other types of insurance policies such as a property, business owners, professional or employer’s liability policy. So, loss of or damage to your business’s property, injuries to your employees, or loss or damage to your customers that do not result from a cyberattack on your business, such as defective products or errors in the advice or services your business provides, and so on, aren’t covered.

**Your obligations if something bad happens - AKA your ‘deductible.’ It is now set at** **$[xxxx]**.

A deductible is an amount that defines your participation in potential monetary loss. It’s called a deductible because it’s deducted from the amount payable under the policy. For example, if you have a covered claim that amounts to $100,000, we will pay you **$[xxxx]** (after we deduct the **$[xxxx]** ‘deductible’). It also means there’s no point in filing a claim with us for less than the **$[xxxx]** deductible.

Opting for a higher deductible means you’re taking more of the risk on yourself, so it is often a way to lower your premium payments. Your business can increase or decrease your deductible. It’s up to you.

**Your obligations if something bad happens - You are required to take immediate steps to minimise loss or damage, notify us right away, and help with our investigation.**

If you willingly handed your business’ computer network, website, data, or records to someone else to manage under contract, they’re ultimately responsible. So, if your business’ data or records were lost, damaged or stolen while under someone else’s care and we pay a loss under this Policy – we will seek reimbursement from them on your behalf. You must provide us with any help we need to do so.

**And more specifically...**

You must notify us promptly of any damage or loss by calling the Waratah Hotline immediately and cooperating with any advice our incident response partners provide.

You must take reasonable steps to minimise the damage (e.g., those steps provided to you by our incident response partners (for example, turning off your computers in the event of a ransomware attack).

You must make a claim under any other policy of insurance that might apply to losses covered under this policy and provide us with those policies.

You must provide us or our partners with the information and records we ask for as soon as possible (e.g., contact information for parties that may be involved, details of any ransomware demand).

We may ask you to submit to examination under oath or provide evidence or affidavits relating to your claim. We may also ask you to take other reasonable steps to ensure we have complete and truthful accounts of the loss and its circumstances.

**Failure to provide complete and truthful information at all times, including before you purchase the policy or after a loss, or to comply with these obligations, will be considered a breach of contract and your duty of utmost good faith.**

We may also be obligated to report it to federal and state authorities.

**Some technical stuff, then we’re done!**

**Changes & Additions**

If you request and we approve changes during the year, we will send you a new policy. That policy will apply from that point to the original expiration date.

**Cancellation & Renewal**

Your policy is for the year and will automatically renew until it is cancelled by you or by us, though you can also pay your premium monthly.

If we choose to cancel or not renew this policy, we’ll notify you at **[xxxx]**. We will provide at least 30 days’ notice so you can get a new policy. If that’s not your email, you can change it here. You are free to cancel your policy at any time, and we will return any leftover part of your paid premiums. Also, please note cancellation will only take place from the date you asked us to cancel the policy, and not before.

If you fail to make a payment, we will try to reach you at the email you provided. If you do not pay within 30 days of the due date, your policy will be cancelled immediately.

**When someone else caused your damage**

‘Subrogation’ is a fancy term for when ‘someone else is responsible for your loss.’ If we pay you for a loss under this policy, then you give us the right to pursue the responsible party to recover what we can. If we recover enough money from them, we’ll even send you back part of your deductible.

We can’t promise we’ll collect, but you give us the right to try. If you get reimbursed by someone else, like your credit card company or computer vendor, you agree to return the money we paid you for that loss. No double-collecting!

Hopefully this all made sense and you feel good about your coverage. Please contact us if anything remains unclear, or if you need more coverage than this agreement provides.

We wish you a successful year, but should you encounter any bumps along the way, we’ll do our best to smooth them out.