emergence smarter cyber insurance

Summary of Key Changes - Cyber Event Protection Policy

Summary of Key Changes from CEP-004.3 NZ to CEP-005 NZ

This document provides a summary of changes to the Emergence Cyber Event Protection policy. It follows the sectional layout of the policy. It is not an exhaustive summary, nor does it form part of the policy wording. Emergence policies will be available on the Emergence website.

Please read the policy wording in its entirety for full details of cover and to ensure it meets your requirements.

Important Information	
Policy Reference	**Description**
About our Services	*The Important Information section describes a range of services provided by cyberSuite to* CEP 005 NZ *policyholders when they purchase a policy. These services are at no cost to the policyholder and are optional to the policyholder to use or take up.* About Our Services Emergence provides a range of services to **our policyholders** when they purchase a **policy** from Emergence. These services are at no cost to the **policyholder** and are optional to the **policyholder** to use or take up. The services are provided in conjunction with an Emergence related company cyberSuite Pty Limited**. Policyholders** can also obtain services directly from cyberSuite, that are not provided with the policy, at a cost to the **policyholder**. When the **policy** is issued by Emergence it will be accompanied by a letter which sets out all the services and how **you** can access the services. The services include tips for better cyber security, an hour free consultation to discuss **your** cyber security, ongoing scanning of **your** internet-facing infrastructure to determine vulnerabilities and dark web scanning to determine if **your** data is vulnerable. All of the services are designed to enhance **your** cyber security while **you** remain a **policyholder** with Emergence. **We** will also provide advice to **you** after a claim on how best to secure **your IT**.
Our Cyber Breach Coach Service	*Clarity to confirm the Emergence Cyber Breach Coach service does not erode the policy aggregate and no excess applies.* Our Cyber Breach Coach Service If there is or **you** reasonably suspect there is a **cyber event** in **your business**, which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will provide an Emergence cyber breach coach to investigate and manage the **cyber event**. Incident response provided solely by an Emergence cyber breach coach does not form part of **cyber event response costs**, does not erode the **aggregate** and no **excess** applies to the cyber breach coach service.

emergence smarter cyber insurance

Section A – Losses to Your Business	
Policy Reference	**Description**
Section A – Losses to Your Business	*Modified Section A to include cover for a cyber event or system failure at your business, cyber event or system failure at your IT contractors business and preventative shutdown.* 1. cyber event in your business If a **cyber event** or **system failure** happens at or within **your business** which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **you** the **impact on business costs**. The maximum **we** will pay in any one **policy period** for **system failure** under this Section A is as stated in the **schedule.** 2. cyber event in your IT contractor's business If a **cyber event** or **system failure** happens at or within **your IT contractor's** business, which is first discovered by **you** and notified to **us** during the policy period, then **we** will pay **you** the **impact on business costs**. The maximum **we** will pay in any one **policy period** for **system failure** under this Section A is as stated in the **schedule.** 3. preventative shutdown If a **preventative shutdown** happens during the **policy period** which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **you** a **preventative shutdown allowance**. The **preventative shutdown allowance** is the maximum **we** will pay in any one **policy period** for all **preventative shutdowns** and is stated in **your schedule**. The sublimit is included in and forms part of the **limit** for Section A – Losses to Your Business.

Section B – Loss to Others	
Policy Reference	**Description**
Section B – Loss to Others	*Modified Section B to include cover for a cyber event, multimedia injury or Payment Card Industry liability.* Section B – Loss to Others **We** will pay a **loss** that **you** are legally liable for arising out of a **claim** that is first made against **you** and notified to **us** during the **policy period** because of: 1. a **cyber event**, or 2. **multimedia injury**, or 3. **Payment Card Industry liability** at or within **your business**.

emergence smarter cyber insurance

Section C – Cyber Event Response Costs	
Policy Reference	**Description**
Section C – Cyber Event Response Costs	*Expanded and modified Section C to provide cover for a cyber event in your business, cyber event in your IT contractor's business and cyber event in your data processor's business.* 1. cyber event in your business If there is a **cyber event** at or within **your business**, or **you** reasonably suspect there is a **cyber event** at or within **your business,** which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **your cyber event response costs.** 2. cyber event in your IT contractor's business If there is a **cyber event** at or within **your IT contractor's** business which is first discovered by **you** and notified to **us** during the **policy period,** then **we** will pay **your IT contractor response costs.** 3. cyber event in your data processor's business If there is a **cyber event** at or within **your data processor's** business which is first discovered by **you** and notified to **us** during the **policy period,** then **we** will pay **your data processor response costs.**

Section D – Optional Covers	
Policy Reference	**Description**
Section D - Optional Covers – Non-IT Contingent Business Interruption and System Failure cover	*Contingent Business Interruption has been changed. Cover for a System Failure at your IT Contractors Business is now included under Section A – Losses to your Business.* *Cover for interruption to your business due to a Cyber Event at a non-IT suppliers is covered under Optional Cover – Non-IT Contingent Business Interruption and System Failure. The previous sublimit for this Optional Cover was $250,000. The sublimit is now $100,000.* *Cover for supplier system failure has been added.* *This protects against events at direct non-IT suppliers without the need for the policyholder to nominate which non-IT suppliers.* **We** will pay **you impact on business costs** caused by: a. **supplier outage**, or b. **supplier system failure**. **cyber event** is extended to be a **cyber event** at or within the business of a **supplier**. For the purposes of this cover only, it shall not include a **cyber event** which happens at or within **your business**, or at or within an **IT contractor's** business. **supplier** means a direct external supplier of goods or services to **your business** other than a utility provider or an IT contractor. **supplier IT** means information technology used at or within **your supplier's** business.

	supplier outage means an interruption to **your business** directly arising from an outage at **your supplier** where, in **our** reasonable opinion, the outage has been caused by a **cyber event** at or within the business of such **supplier.** **supplier system failure** means an interruption to **your business** directly arising from an unintentional, unexpected and unplanned outage of **your supplier's IT** but does not include outage: a. caused by a cyber event; b. caused by using untested, disapproved or illegal software, or software that is past its end-of-life and no longer supported; c. caused by use of a non-operational part of the **supplier IT;** d. falling within parameters of a service level agreement; e. arising out of commercial dispute, failure to pay for services or refusal to deliver services paid for; f. arising out of **your IT** or **IT** under the direct operational control of **your IT contractor.**
Section D - Optional Covers – Criminal Financial Loss	*Direct Financial Loss definition expanded to include Cloud usage charges caused by Cryptojacking (d).* **direct financial loss** means a. **your** funds, accounts receivable or securities, or the funds, accounts receivable or securities in **your** control belonging to others, that are lost due to **cyber theft, identity-based theft** or **socially engineered theft** and remain unrecoverable, or b. **your** customers funds that are lost due to **push payment theft** and remain unrecoverable, or c. unintended or unauthorised call charges or bandwidth charges in excess of normal and usual amounts that **you** must pay caused by **telephone phreaking**, or d. unintended or unauthorised bandwidth charges, electricity costs, or cloud usage charges in excess of normal and usual amounts that **you** must pay caused by **cryptojacking**. **Direct financial loss** does not include digital currencies, gift cards, vouchers, coupons or reward points.
Section D - Optional Cover – D&O Liability Cover	*Section D – Optional Cover to include D&O Liability. This is a new cover.* **We** will pay a **loss** that any of **your** directors or officers is legally liable for arising out of a **claim** that is first made against **your** directors or officers and notified to **us** during the **policy period** because of a **cyber wrongful act** in **your business.** **claim** means any written demand, notice of pending action or civil, criminal, administrative, regulatory or arbitral proceedings against **your** directors or officers seeking compensation or other legal remedy caused by or in connection with a **cyber wrongful act**. **cyber wrongful act** means an act, error, omission, breach of duty, or neglect directly arising out of a covered **cyber event** that leads to the personal liability of any of **your** directors or officers that is not otherwise insured and that **you** do not otherwise indemnify.

	See policy wording for D&O definitions and exclusions.
Section D - Optional Cover – Tangible Property	*Expanded cover - Tangible Property sublimit now is increased to be the same limit as Section C – Cyber Event Response Costs.* **We** will pay the cost of the replacement or repair of **your IT** hardware at or within **your business** that is physically damaged or no longer suitable for use solely and directly because of a **cyber event** covered under this **policy** or the incurring of related **cyber event response costs.** The sublimit for Tangible Property Cover forms part of, and is not in addition to, the **limit** for Section C - Cyber Event Response Costs.

Section E - What Certain Words Mean	
Policy Reference	**Description**
Claim	*Definition expanded to include Payment Card Industry Liability.* **claim** means any written demand, notice of pending action or civil, criminal, administrative, regulatory or arbitral proceedings against **you** seeking compensation or other legal remedy caused by or in connection with a **cyber event, multimedia injury** or **Payment Card Industry liability.**
Cyber Event Response	*Modified definition of Public Relation Costs.* **public relations costs** incurred in responding to a **cyber event**, or adverse media arising from a **cyber event**, including external public relations, media, social media and communications management to prevent reputational harm to **you.** *New definition for IT Forensic Costs.* **IT forensic costs** incurred by **you** with **our** prior consent, to investigate a **cyber event** or suspected **cyber event**.
Data Processor	*New definition for coverage under Section C – Cyber Event Response Costs.* **Data processor** means a person other than an **IT contractor** who processes **your** data under a contract with **you**.
Data Processor Response Costs	*New definition for coverage under Section C – Cyber Event Response Costs.* **data processor response costs** means the reasonable and necessary costs and expenses **you** incur in responding to a **cyber event** at or within **your data processor's** business that impacts **your** data being: **- credit and identity monitoring costs,** **- cyber extortion costs,** **- data restoration costs,** **- data securing costs,** **- external management costs,** **- identity theft response costs,** **- legal advice costs,**

	- notification costs and **- public relations costs**. **data processor response costs** does not mean the **data processor's** own costs.
IT	*New definition for IT simplifies and replaces the previous definition of IT Infrastructure.* **IT** means all of the hardware, servers, systems, firmware, software, networks, platforms, facilities owned by, leased to, rented to or licensed to: a. **you**, or b. **your IT contractor** insofar and solely as they are required to develop, test, deliver, monitor, control or support information technology services you use in **your business**. The term **IT** includes all of the information technology, but not the associated people, processes and documentation.
IT Contractor	*The definition of IT Contractor has changed to align with the coverage under Sections A and C.* **IT** contractor means a business **you** do not own, operate or control, but that **you** hire under contract to provide, maintain, service or manage information technology services on **your** behalf that are used in **your business.**
IT Contractor Response Costs	*New definition for* coverage under Section C – Cyber Event Response Costs. **IT contractor response costs** means the reasonable and necessary costs and expenses you incur in responding to a **cyber event** at or within **your IT contractor's** business that impacts **your** data being: **- credit and identity monitoring costs,** **- cyber extortion costs,** **- data restoration costs,** **- data securing costs,** **- external management costs,** **- identity theft response costs,** **- legal advice costs,** **- notification costs and** **- public relations costs**. **IT contractor response costs** does not mean the **IT contractor's** own costs.
System Failure	*New definition for coverage under Section A – Losses to your Business.* **system failure** means an interruption to **your business** directly arising from an unintentional, unexpected and unplanned outage of **IT**, but does not include outage: a. caused by a **cyber event;** b. caused by using untested, disapproved or illegal software, or software that is past its end-of-life and no longer supported; c. caused by use of a non-operational part of IT; d. falling within parameters of a service level agreement;

	e. arising out of commercial dispute, failure to pay for services or refusal to deliver services paid for. The waiting period for **system failure** is stated in **your schedule**.

Section F - Exclusions

Policy Reference	Description
Exclusion 7	*Previous Exclusions 7, 8 and 12 have become consolidated into Exclusion 7.* a. ionising, radiation or contamination by radioactivity from any nuclear fuel, waste or other hazardous properties of any nuclear assembly or component, b. pollution, c. any electromagnetic field, electromagnetic radiation or electromagnetism.
Exclusion applicable to Section B only	*The previous exclusion (27 b.) for claims arising out of errors or omissions while acting in a professional capacity has been removed.* *Exclusion 27 c no longer applies to IT contractors. As the definition to IT Contractors has changed, this exclusion is now limited to the failure of IT services.* Exclusions – policy Section B only The following exclusions apply to Section B only. **We** will not pay a **loss** that **you** are legally liable for arising out attributable to or as a consequence of a **claim** under Section B of the **policy**: 23. for an action: a. brought against **your** directors or officers acting in that capacity, or b. brought against **you** as a result of any failure of information technology services provided, maintained, serviced or managed by **you** for a third party for a fee as part of **your business activities.** *Former exclusion 28 relating to IT products, services or infrastructure provided to others has been removed and replaced by a straightforward products exclusion.* 24. in connection with any products, including packaging, labelling or instructions, that **you** design, assemble, manufacture, distribute, service, sell, rent, lease or license to others for a fee.

Section G - Claims Conditions

Policy Reference	Description
Condition 15	*Condition modified* if **you** suffer a **direct financial los**s as a result of **cyber theft**, s**ocially engineered theft, identity-based theft or push payment theft** and **you** are actively pursuing the recovery of the funds through **your** financial institution **we** will pay the claim within 30 days of the claim being notified to **us. You** must cooperate with and assist **us** in our attempts to

	recover **your direct financial loss** and **you** must reimburse **us** for any funds recovered by **you.**

Section H – General Conditions	
Condition 24	*Previous Sanctions Exclusion is now a General Condition.* Sanctions Limitation Clause No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)insurer to any sanction, prohibition or restriction under United Nations' resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom, United States of America or any trade or economic sanctions, laws or regulations of any other jurisdiction.

Emergence NZ Limited (NZBN: 9429051153861, FSP: 1005174) ('Emergence') acts under a binding authority given to it by certain Underwriters at Lloyd's.

More information on Emergence can be found on our website: www.emergenceins.co.nz

You can contact us at:
Email: info@emergenceins.co.nz
Telephone: 0800 129 237 (0800 1 CYBER)