emergence

summary of key changes

This document provides a summary of changes to the Emergence Cyber Enterprise Solution policy. It follows the sectional layout of the policy. It is not an exhaustive summary of the entire policy, nor does it form part of the Policy Wording. All Emergence policies are available on the Emergence website.

IMPORTANT INFORMATION

POLICY REFERENCE	DESCRIPTION
About our Services	*The Important Information section has been updated to confirm we offer a range of services to our CES 003 policyholders when they purchase a policy with us. These services are either at no cost to the policyholder or offered at a discounted rate and are completely optional for 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 either at no cost to the **policyholder** or offered at a discounted rate and are optional to the **policyholder** to use or take up. 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 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 computer systems**.
Our Cyber Incident Response Service	*The Important Information section has been updated to reaffirm that our Emergence Incident Response service does not erode the policy aggregate and no excess applies (per Section D – Extensions).* Our Cyber Incident Response Service If there is or **you** reasonably suspect there is a **cyber event** happening to **your business**, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, then **we** will provide an Emergence incident responder to investigate and manage the **cyber event**. Incident response provided solely by an Emergence incident responder does not form part of **cyber event response costs**, does not erode the **aggregate** and no **excess** applies to the cyber incident response service.

emergence

summary of key changes

IMPORTANT INFORMATION

POLICY REFERENCE	DESCRIPTION
How to notify us if a cyber event happens or a claim is made against you	*The Important Information section has been updated to include an overview of how to notify us of a cyber event or claim.* How to notify us if a cyber event happens or a claim is made against you: 1. **You** must immediately ring the Emergence cyber event reporting line on 1300 799 562 or notify Emergence in writing at **claims@emergenceinsurance.com.au** and provide details and circumstances of the event, including any **claims**, demands or notices received by **you** or proceedings against **you**. 2. **You** must report **telephone phreaking** or **cryptojacking** to, respectively, the Australian Cyber Security Centre, **your** financial institution, and **your** telephone service provider or utility provider, within 24 hours of it first being discovered by **your senior management team**. 3. **We** will assess whether cover applies under **your policy**. 4. **You** must do everything reasonably possible to preserve evidence to enable **us** to properly assess and investigate the claim. 5. If the claim is not covered under **your policy**, **we** will advise **you** to engage **your** own service resources. This is a quick reference provided for **your** convenience. Please refer to Section H of the **policy** for a full listing of Claims Conditions.
General Insurance Code of Practice	*The important information section has been updated to provide further information for our Policyholders around the General Insurance Code of Practice and external resources available:* The Insurance Council of Australia Limited has developed the General Insurance Code of Practice ("the Code"), which is a voluntary self-regulatory code. The Code aims to raise the standards of practice and service in the insurance industry. Lloyd's has adopted the Code on terms agreed with the Insurance Council of Australia. For further information on the Code please visit www.codeofpractice.com.au The Code Governance Committee (CGC) is an independent body that monitors and enforces insurers' compliance with the Code. For more information on the Code Governance Committee (CGC) go to www.insurancecode.org.au.

emergence

summary of key changes

SECTION A – BUSINESS INTERRUPTION

POLICY REFERENCE	DESCRIPTION
Section A – Business Interruption	*Modified previous Section A - Business Interruption and Section B - Dependant Business Interruption into a combined Section A – Business Interruption to outline our business interruption cover includes a cyber event at or within your business, at or within your IT contractor's business and voluntary shutdown (previously preventative shutdown). We also replaced system outage with outage (as the definition of system outage was deemed redundant) and introduced the waiting period into the insuring clause.* 1. cyber event in your business If a **cyber event** happens at or within **your business**, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, and that **cyber event** causes an **outage** which exceeds the **waiting period**, then **we** will pay **you impact on business costs**. **We** will not pay i**mpact on business costs** during the **waiting period**. The maximum amount **we** will pay in any one **policy period** is the **limit** as stated in **your schedule**. 2. cyber event in your IT contractor's business If a **cyber event** happens at our within **your IT contractor's** business, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, that causes an **outage** in **your** business which exceeds the **waiting period**, then **we** will pay **you impact on business costs**. **We** will not pay **impact on business costs** during the **waiting period**. The maximum amount **we** will pay in any one **policy period** is the **limit** as stated in **your schedule**. 3. voluntary shutdown If a **voluntary shutdown** which exceeds the **waiting period** happens at or within **your** business, during the **policy period**, and notified to **us** during the **policy period**, **we** will pay **you voluntary shutdown allowance**. **We** will not pay **voluntary shutdown allowance** during the **waiting period**. The **voluntary shutdown allowance** is the maximum **we** will pay in any one **policy period** for all **voluntary shutdown** and the sub limit is as stated in **your schedule**. This sub limit shall form part of the **limit** for Section A – Business Interruption. The maximum **we** will pay in any one **policy period** for Section A – Business Interruption, is the **limit** stated in **your schedules**.

emergence

summary of key changes

SECTION B – CYBER & PRIVACY LIABILITY

POLICY REFERENCE	DESCRIPTION
Section B – Cyber & Privacy Liability	*Expanded and modified Section B to clarify intent to provide cover for losses our insured is legally liable for arising out of a claim made against them due to a cyber event at or within their business, at or with their IT contractor's business, at or within their data processor's business and payment card industry liability. Previously endorsed to the policy.* **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**, if such **claim** was made against **you** due to: 1. a **cyber event** at or within **your business**; or 2. a **cyber event** at or within **your IT contractor's** business; or 3. a **cyber event** at or within **your data processor's** business; or 4. **payment card industry liability** which is first discovered by **your senior management team** and notified to **us**. The maximum **we** will pay in any one **policy period** for Section B – Cyber and Privacy Liability, is the **limit** as stated in **your schedule**.

SECTION C – CYBER EVENT RESPONSE COSTS

POLICY REFERENCE	DESCRIPTION
Section C – Cyber Event Response Costs	*Expanded and modified Section C to clarify intent to cover response costs incurred by our insured in responding to a cyber event that has occurred at or within their IT contractor's business or at or within their data processor's business by introducing IT contractor response costs and data processor response costs. Previously endorsed to the policy.* 1. cyber event to your business If a **cyber event** happens at or within **your business**, or **you** reasonably suspect there is a **cyber event** happening at or within **your business**, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, then **we** will pay **your cyber event response costs**. 2. cyber event to your IT contractor's business If a **cyber event** happens at or within to **your IT contractor's** business, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, **we** will pay **your IT contractor response costs**.

emergence

summary of key changes

SECTION C – CYBER EVENT RESPONSE COSTS

POLICY REFERENCE	DESCRIPTION
	3. cyber event to your data processor's business If a **cyber event** happens at or within **your data processor's** business, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, **we** will pay **your data processor response costs**. The maximum **we** will pay in any one **policy period** for Section C – Cyber Event Response Costs, is the **limit** as stated in **your schedule**.

SECTION D – EXTENSIONS

POLICY REFERENCE	DESCRIPTION
emergence incident responder	*Replaced cyber breach coach with incident responder and modified 'a cyber event in your business' to 'a cyber event happening to your business' to clarify intent that an Emergence incident responder can support our Insureds even if the cyber event impacting them has occurred at or within their IT contractor's business or at or within their data processor's business.* If **there** is, or **you** reasonably suspect there is, a **cyber event** happening to **your business**, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, then **we** will provide an Emergence incident responder to investigate and manage the **cyber event**. Incident response provided solely by the Emergence incident responder does not form part of **cyber event response costs**, does not erode the **aggregate** and no **excess** applies.
betterment costs	*Modified to include at or within your business to align with the revisions made in Section A – Business Interruption.* If there is a **cyber event** at or within **your business** which is first discovered by **your senior management team** and notified to **us** during the **policy period**, then **we** will pay the additional cost and expenses to replace or restore **your** software with newer, upgraded, and/or improved versions of the impacted software. The maximum **limit we** will pay is twenty percent (20%) more than the cost would have been to repair or replace the original version of the software, or the sublimit stated in **your schedule**, whichever is the lesser.

emergence

summary of key changes

SECTION D – EXTENSIONS

POLICY REFERENCE	DESCRIPTION
claims preparation costs	*Modified to confirm claims preparation costs include assistance in verifying voluntary shutdown allowance and reputational harm impact.* **We** will pay for claims preparation costs incurred with **our** prior written consent for a third party to assist **you** to verify **impact on business costs**, **voluntary shutdown allowance or reputational harm impact** incurred by **you**. **We** will pay up to the sublimit stated in **your schedule** for Section D – claims preparation costs.

SECTION E - OPTIONAL COVERS

POLICY REFERENCE	DESCRIPTION
reputational harm	*Modified to clarify the reputational harm sublimit forms part of the limit for Section A – Business Interruption.* If an **adverse media event** happens involving **your business** which is first discovered by **your senior management team** and notified to us during the policy period, then **we** will pay **you** the **reputational harm impact**. The maximum **we** will pay in any one **policy period** for Optional Cover – reputational harm is the sublimit as stated in **your schedule**. This sublimit forms part of the **limit** for Section A – Business Interruption.
system failure	*Modified to align with the structure of Section A – Business Interruption by splitting out system failure and dependant business system failure, clarify it forms part of the limit for Section A – Business Interruption and we now rely on the standard definition of indemnity period which is referenced within the schedule rather than a fixed number of days.* **We** will pay **you impact on business costs** solely as a result of a **system failure** at or within **your business**, which exceeds the **waiting period**, which is first discovered by **your senior management team** and notified to **us** during the **policy period**. **We** will not pay **impact on business costs** during the **waiting period**. The maximum **we** will pay in any one **policy period** for Optional Cover – system failure is the sub limit as stated in **your schedule**. This sub limit forms part of the **limit** for Section A – Business Interruption.

emergence

summary of key changes

SECTION E - OPTIONAL COVERS

POLICY REFERENCE	DESCRIPTION
dependent business system failure	*New optional cover introduced to align with structure of Section A – Business Interruption.* **We** will pay **you impact on business costs** solely as a result a **system failure** at or within **your IT contractor's** business, which exceeds the **waiting period**, which is first discovered by **your senior management team** and notified to **us** during the **policy period**. **We** will not pay **impact on business costs** during the **waiting period**. The maximum **we** will pay in any one **policy period** for Optional Cover – dependent business system failure is the sub limit as stated in **your schedule**. This sub limit forms part of the **limit** for Section A – Business Interruption.
multimedia liability	*Modified to clarify the multimedia liability sublimit forms part of the limit for Section B – Cyber & Privacy Liability.* **We** will pay a **loss** that **you** are legally liable for arising out of a **multimedia claim** that is first made against **you** and notified to **us** during the **policy period** because of **multimedia injury**. Section G – Exclusion 8 of the **policy** is not applicable to any **multimedia claim** under the **policy** pursuant to this Optional Cover – multimedia liability. The maximum **we** will pay in any one **policy period** for Optional Cover – multimedia liability is the sublimit as stated in **your schedule**. This sublimit forms part of the **limit** for Section B – Cyber & Privacy Liability.
tangible property	*Modified to clarify that the tangible property sublimit forms part of the limit for Section C – Cyber Event Response Costs and modified tangible property to expand cover to include servers.* **We** will pay the cost of the replacement or repair of **your** IT hardware that is 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**, provided that replacing or repairing **your** IT hardware is more cost effective than installing new firmware or software onto **your** existing IT hardware. **We** will not pay any cost to replace or repair: a. IT hardware that is physically stolen, lost, or damaged; or b. **operational technology** Section G – Exclusion 1 of the **policy** is not applicable to any claim under the **policy** pursuant to this Optional Cover – tangible property cover. The maximum **we** will pay in any one **policy period** Optional Cover – tangible property, is the sublimit as stated in **your schedule**. This sublimit forms part of the limit for Section C – Cyber Event Response Costs.

emergence

summary of key changes

SECTION E - OPTIONAL COVERS

POLICY REFERENCE	DESCRIPTION
joint venture and consortium	*Modified to clarify the joint venture and consortium sublimit forms part of the limit for Section B – Cyber & Privacy Liability and update the information requirement from declared revenue from coming 12 months to preceding 12 months to align with our standard rating methodology for the broader placement.* The cover provided under Section B – Cyber & Privacy Liability section of this **policy** is extended to **your** participation in a joint venture or consortium **you** have declared to **us**. This Optional Cover – joint venture and consortium applies only if **you** have declared to **us** the total revenue received from the joint venture or consortium during the preceding twelve (12) month period and the joint venture or consortium is named in **your schedule**. This Optional Cover covers **you** only. No other participant in such joint venture or consortium, and no other third party, has any rights under this **policy**, nor shall **we** be liable to pay a contribution to any insurer of any other participant in such joint venture or consortium. Section G – Exclusion 15 of the **policy** is not applicable to any **claim** under the **policy** pursuant to this Optional Cover – joint venture and consortium. The maximum **we** will pay in any one **policy period** or Optional Cover – joint venture and consortium is the sublimit as stated in **your schedule**. This sublimit forms part of the **limit** for Section B – Cyber & Privacy Liability.

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
claim	*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** by a third party seeking compensation or other legal remedy as a consequence of or in connection with a **cyber event** or **payment card industry liability**. **Claim** does not include a **multimedia claim**.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
computer system	*Modified to simplify and combine the previous definitions of 6. computer system 7. computer systems and 23. IT Infrastructure and to add reference to a data processor's computer systems.* **computer system** means: a. all of the hardware, firmware, software, networks, servers, systems, platforms, facilities owned by, leased to, rented to, or licensed to: i. **you**; or ii. **your IT contractor**; or iii. a **data processor** in respect of Section B.3 and C.3 only, insofar as they are required to develop, test, deliver, monitor, control or support information technology services **you** use in **your business**; and b. **operational technology**. The term **computer system** includes all of the information technology, but not the associated people, processes, and documentation. For the purpose of exclusion 9 only, **computer system** means: any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.
cyber event	*Modified to remove "your" from "your computer systems" within a. – g. and i. l. to align with the cover under Sections A – D, omitted the attribution requirement of a security compromise or unauthorised access of data from f. insider and privilege misuse, introduced data processor to h. privacy error, replaced IT Infrastructure with computer systems within i. payment card skimming, j. physical theft and loss and l. web app attacks.* **cyber event** means any of the following: a. **crimeware** which is any malware of any type intentionally designed to cause harm to **computer systems** but does not include **cyber espionage** or **point of sale intrusion**. b. **cyber espionage** which is unauthorised access to an item of **computer systems** linked to a state affiliated or criminal source exhibiting the motive of espionage.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
	c. **cyber extortion** which is a crime involving an attack or threat of attack against **computer systems**, or data in **computer systems**, coupled with a demand for money or other valuable consideration (including digital currency) to avert or stop the attack. d. **denial of service** which is intended to uniquely compromise the availability of **computer systems**. This includes a distributed **denial of service**. e. **hacking** which is malicious or unauthorised access to **computer systems**. f. **insider and privilege misuse** which is unapproved or malicious use of **computer systems** by employees, outsiders in collusion with employees, or business partners who are granted privilege access to **computer systems**. g. **miscellaneous errors** which is where unintentional action(s) directly compromise(s) a security attribute of an item of **computer systems**. h. **payment card skimming** which is where a skimming device is physically implanted through tampering into an item of **computer systems** and that skimming device reads data from a payment card. i. **physical theft** and loss which is where an item of **computer systems** is missing or falls into the hands of a third party or the public, whether through misplacement or malice. j. **point of sale intrusion** which is a remote attack against **computer systems** where retail transaction purchases are made by a payment card. k. **privacy error** which is where unintentional act(s) or omission(s) by **your** employee(s), **your data processor(s)** or **your IT contractor(s)** lead(s) to unauthorised access to, unauthorised disclosure of or loss of **your** data or data **you** hold on behalf of third parties in connection with the **business** (including non-electronic data). l. **web app attacks** which is where a web application was the target of an attack against **computer systems**, including exploits of code level vulnerabilities in the application.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
cyber event response costs	*Introduced call centre costs, modified crisis management costs to provide greater clarity on intent and replaced identity theft response costs with identification replacement costs to provides affirmative language for ID replacement costs.* a. **call centre costs** which means costs to establish and operate a call centre to provide information to any person whose data or information has been accessed or lost. c. **crisis management costs** which means external management costs incurred in responding to a **cyber event**, including crisis management and mitigation measures engaged in by **you** and agreed to by **us**, when necessary to counter a credible impending threat to stage a **cyber event** against **computer systems** and to prevent reputational harm to **you**. g. **identification replacement costs** which means costs to support an individual, whose data or information has been accessed or lost through a **cyber event**, with re-establishing identity and essential records. Such costs shall include those incurred for the replacement of official identification documents, where such replacement is: a. enforced by a regulatory body, or b. will mitigate a larger loss already covered by this **policy**.
data processor	*New definition introduced for cover under Section C.3 - cyber event in your data processor's business. Previously endorsed to the policy.* **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 introduced for cover under Section C.3 - cyber event in your data processor's business. Previously endorsed to the policy.* **data processor response costs** means the reasonable and necessary costs and expenses **you** incur with **our** prior consent, in responding to a **cyber event** that happens to **your data processor's business** and impacts **your** data, being: a. **call centre costs** which means costs to establish and operate a call centre to provide information to any person whose data or information has been accessed or lost.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
	b. **credit and identity monitoring costs** which means costs to engage monitoring services by a third party for persons affected by a **cyber event** for a period of up to twelve (12) months. c. **crisis management costs** which means external management costs incurred in responding to a **cyber event**, including crisis management and mitigation measures engaged in by **you** and agreed to by **us**, when necessary to counter a credible impending threat to stage a **cyber event** against **computer systems** and to prevent reputational harm to **you**. d. **cyber extortion costs** which means costs to respond to a **cyber event** where a third party is seeking to obtain pecuniary gain from **you** through **cyber extortion**. e. **data restoration costs** which means costs to: i. restore or replace **your** data or programs in **computer systems** that have been lost, damaged, or destroyed; ii. mitigate or prevent further damage; and iii. purchase replacement licenses, if necessary. **data restoration costs** does not include any costs to redesign, replicate or reconstitute proprietary information, facts, concepts, or designs. f. **data securing costs** which means costs to secure **computer systems** to avoid ongoing **loss**, and **data processor response costs**. g. **identification replacement costs** which means costs to support an individual, whose data or information has been accessed or lost through a **cyber event**, with re-establishing identity and essential records. Such costs shall include those incurred for the replacement of official identification documents, where such replacement is: i. enforced by a regulatory body; or ii. will mitigate a larger loss already covered by this **policy**. h. **legal costs** which means costs to retain legal or regulatory advice in relation to **your** rights and obligations in respect of any legal and regulatory issues that arise as a result of a **cyber event**. **Legal costs** do not include **defence costs**. i. **notification costs** which means costs to notify any person whose data or information has been accessed or lost, including the cost of preparing a statement to the Office of the Australian Information Commissioner or other authorities.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
	j. **public relations costs** which means external public relations, media, social media, communications management and similar costs to avoid or mitigate reputational harm to **your business** as a consequence of a **cyber event**. **data processor response costs** does not mean the **data processor's** own costs.
delayed net profit	*New definition introduced to reinforce that net profit delayed is not net profit lost.* **delayed net profit** means **net profit** earned in the period of ninety (90) days after the end of the **indemnity period** which would have been earned during the **indemnity period** if the **cyber event**, **system failure**, **voluntary shutdown** or **adverse media event** did not happen.
employee wrongful act	*Modified the employee wrongful act exclusion by including a write back for employee data impacted by a cyber event.* **employment wrongful act** means any actual or alleged employment-related act, error, omission or conduct constituting actual, constructive or alleged: wrongful dismissal, discharge or termination of employment; wrongful failure to employ or promote; wrongful deprivation of career opportunity; misleading representation or advertising in respect of employment; wrongful disciplinary action; negligent employee evaluation; wrongful demotion; failure to pay salary or any other employment-related benefits; breach of employment contract; sexual or workplace harassment (including the creation of a workplace environment conducive to such harassment); wrongful discrimination; failure to grant tenure; invasion of privacy or defamation. **Employment wrongful act** does not mean employee data impacted by a **cyber event**.
identity theft	*Deleted previous definition 16 due identify theft response costs being replaced with identification replacement costs.*

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
impact on business costs	*Modified point a. of impact on business costs to replace 'less any net profit that is subsequently recouped within a reasonable additional time period (which is not limited to the indemnity period)' with 'delayed net profit' to provide greater clarity on what is deemed reasonable additional time and further clarify that impact on business costs does not include IT contractor response costs, reputational harm impact and voluntary shutdown allowance.* **impact on business costs** means: a. the amount that the **net profit you** earn during the **indemnity period** falls short of the **net profit you** ordinarily earn, solely and directly as a result of a **cyber event** or **system failure**, less any **delayed net profit** and less any consequent savings by **you**; b. the net increased costs **you** incurred during the **indemnity period** to avoid or mitigate a reduction in **your net profit** directly as a result of a **cyber event** or **system failure**, provided the amount of increased cost paid is less than **we** would have paid for a reduction in standard **net profit** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries, or overhead expenses. **Impact on business costs** does not include **cyber event response costs**, **IT contractor response costs**, **reputational harm impact** and **voluntary shutdown allowance**.
indemnity period	*Modified to expand the definition to include system failure and 'plus reasonable additional time to allow for your business to normalise' to provide clarity on existing intent.* **indemnity period** means the period starting from discovery of the **cyber event** or **system failure**, and lasting until **computer systems** are restored to their usual function, plus reasonable additional time to allow for **your** business to normalise, however in total length, not exceeding the number of days set out in **your schedule**.
IT contractor	*Modified the definition of IT contractor to align with the cover under Sections A.2 cyber event in your IT contractor's business, Section B – Cyber & Privacy Liability and Section C – Cyber Event Response Costs.* **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**.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
IT contractor response costs	*New definition introduced for cover under Section C.2 - cyber event in your IT contractor's business. Previously endorsed to the policy.* **IT contractor response costs** means the reasonable and necessary costs and expenses **you** incur with our prior consent, in responding to a **cyber event** that happens to **your IT contractor's** business and impacts **your** data, being: a. **call centre costs** which means costs to establish and operate a call centre to provide information to any person whose data or information has been accessed or lost. b. **credit and identity monitoring costs** which means costs to engage monitoring services by a third party for persons affected by a **cyber event** for a period of up to twelve (12) months. c. **crisis management costs** which means external management costs incurred in responding to a **cyber event**, including crisis management and mitigation measures engaged in by **you** and agreed to by **us**, when necessary to counter a credible impending threat to stage a **cyber event** against **computer systems** and to prevent reputational harm to **you**. d. **cyber extortion costs** which means costs to respond to a **cyber event** where a third party is seeking to obtain pecuniary gain from **you** through **cyber extortion**. e. **data restoration costs** which means costs to: i. restore or replace **your** data or programs in **computer systems** that have been lost, damaged, or destroyed; ii. mitigate or prevent further damage; and iii. purchase replacement licenses, if necessary. **data restoration costs** does not include any costs to redesign, replicate or reconstitute proprietary information, facts, concepts, or designs. f. **data securing costs** which means costs to secure **computer systems** to avoid ongoing **impact on business costs**, **loss**, and **IT contractor response costs**. g. **identification replacement costs** which means costs to support an individual, whose data or information has been accessed or lost through a **cyber event**, with re-establishing identity and essential records. Such costs shall include those incurred for the replacement of official identification documents, where such replacement is: iv. enforced by a regulatory body; or v. will mitigate a larger loss already covered by this **policy**.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
	h. **legal costs** which means costs to retain legal or regulatory advice in relation to **your** rights and obligations in respect of any legal and regulatory issues that arise as a result of a **cyber event. Legal costs** do not include **defence costs**. i. **notification costs** which means costs to notify any person whose data or information has been accessed or lost, including the cost of preparing a statement to the Office of the Australian Information Commissioner or other authorities. j. **public relations costs** which means external public relations, media, social media, communications management and similar costs to avoid or mitigate reputational harm to **your business** as a consequence of a **cyber event**. **IT contractor response cost**s does not mean the **IT contractor's** own costs.
limit	*Modified the definition of limit to include defined events.* **limit** means the amount set out in **your schedule** for each of Section A – Business Interruption, Section B – Cyber & Privacy Liability and Section C – Cyber Event Response Costs of **your policy** and applies to any one **cyber event**, **voluntary shutdown**, **claim**, **adverse media event**, **system failure**, or **multimedia claim** irrespective of the number of claim(s). The sublimit for any Optional Cover is also set out in **your schedule**.
multimedia claim	*Modified to include "by a third party" ahead of seeking compensation and replaced "…caused by or in connection…" with "as a consequence of or in connection with…" to maintain consistency across the definition of claim and multimedia claim.* **multimedia claim** means any written demand, notice of pending action or civil, criminal, administrative, regulatory, or arbitral proceedings against **you** by a third party seeking compensation or other legal remedy and as a consequence of or in connection with a **multimedia injury**.
multimedia injury	*Modified the definition of multimedia injury to omit previous point d. non-conformance with any legal requirement relating to web access such as the Disability Discrimination Act of 1992 as this scope of cover is more appropriately addressed by a stand-alone multimedia liability policy.* **multimedia injury** means loss to others because of unintentional: a. libel, slander, defamation;

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
	b. infringement of trademark, service mark, slogan, copyright, domain name or meta tags; c. improper deep linking, framing, or web harvesting; d. inadvertent disclosure of personal information; but only to the extent that the loss is solely occasioned by **your** website content, social media presence (including comments made by third parties for which **you** may be held legally responsible) or other online mediums. **multimedia injury** does not include any actual or alleged infringement by **you** of any patent.
operational technology	*The reference to IT Infrastructure has been removed from the definition of operational technology.* **operational technology** means hardware and software used to monitor or control physical processes and industrial operations in **your business** and includes Industrial Controls Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Internet of Things (IOT).
outage	*Modified to replace "your computer systems" with "computer systems" to ensure cover aligns with Sections A.1 and A.2.* **outage** means the disruption or degradation of, disturbance to, or an inability to access **computer systems**.
preventative shutdown	*Deleted previous definition 35 as it has been replaced with the new definition voluntary shutdown.*
preventative shutdown allowance	*Deleted previous definition 36 as it has been replaced with the new definition voluntary shutdown allowance.*
regulatory shutdown	*New definition introduced for cover under Section A.1 – cyber event to your business or Section A.2 – cyber event to your IT contractor's business.* **regulatory shutdown** means the reasonable and necessary shutdown of **your computer systems** where such action has been ordered by a government or regulatory authority solely due to a confirmed **cyber event** which is reasonably expected to impact **your business**.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
reputational harm impact	*Modified point a. of reputational harm impact to replace 'less any net profit that is subsequently recouped within a reasonable additional time period (which is not limited to the indemnity period)' with 'delayed net profit' to provide greater clarity on what is deemed reasonable additional time and clarify reputational harm impact does not include data processor response costs, IT contractor response costs, impact on business costs and voluntary shutdown allowance.* **reputational harm impact** means: a. the amount that the **net profit you** earn during the **reputational harm period** falls short of the **net profit you** ordinarily earn solely and directly as a result of an **adverse media event**, less **delayed net profit** and any consequent savings, and b. the net increased costs incurred to avoid a reduction in **net profit** directly as a result of an **adverse media event** provided the amount of increased cost paid is less than **we** would have paid for a reduction in standard **net profit** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries, or overhead expenses. **reputational harm impact** does not include **cyber event response costs**, **data processor response costs**, **IT contractor response costs**, **impact on business costs** and **voluntary shutdown allowance**.
reputational harm period	*Modified to remove the fixed 60-day reputational harm period and reputational harm period will now be referenced within the schedule.* **reputational harm period** means the number of consecutive days stated in **your schedule**, starting from the date of the first publication of an **adverse media event**.
system failure	*Modified to simply and remove the deleted definition of IT Infrastructure.* **system failure** means an unintentional, unexpected, and unplanned **outage**, but does not include an **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 **computer systems**; or d. arising out of commercial dispute, failure to pay for services or refusal to deliver services paid for.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
system outage	*Deleted previous definition 44 as it was deemed redundant and instead will rely on the definition of outage.*
utility provider	*Internet access, internet backdone, DNS services or other core infrastructure of the internet has been omitted from the definition of utility provider as it is now addressed seperately in point c. of exclusion 13.* *The write-back for services under your direct control has been omitted from this definition and instead introduced within exclusion 13.* **utility provider** means the providers of gas, electricity, water, sewage, telecommunications, satellite and cable.
voluntary shutdown	*New definition introduced for coverage under Section A.3 - voluntary shutdown. Previously preventative shutdown. Language largely aligns to previous definition of preventative shutdown however we have replaced IT infrastructure with computer systems.* **voluntary shutdown** means the reasonable, necessary, and intentional shutdown of **your computer systems** carried out, approved by or directed by a member of **senior management team**, in response to a known, reasonably suspected or credible threat to **your computer systems** which is first discovered by **your senior management team** and notified to **us** during the **policy period**, following: a. a **cyber event** to the **computer systems** of **your** direct customer, supplier, or business partner; b. a specific instruction from **your** financial institution, law enforcement or the Australian Signals Directorate or similar agency of the government; or c. a communication by a third party threatening to carry out **cyber extortion**, a **denial of service** attack or other **cyber event** to **your computer systems**; and where such action will mitigate, reduce or avoid an otherwise larger claim under this **policy**. **voluntary shutdown** does not include shutdown due to: a. routine maintenance; b. patching or updating of software; c. use of software that is past its end-of- life and no longer supported; d. intentional shutdown of an **IT contractor's computer systems** or **data processor's computer systems**; or e. for any reason other than mitigation of threat to **your computer system** or avoidance of otherwise larger claims under this **policy**.

emergence

summary of key changes

SECTION F – DEFINITIONS

POLICY REFERENCE	DESCRIPTION
voluntary shutdown allowance	*New definition introduced for coverage under Section A.3 – voluntary shutdown. Language aligns to previous preventative shutdown allowance definition with a modification to introduce a mechanism for further coverage beyond the initial 72 hours covered.* If, after seventy-two (72) consecutive hours, a **cyber event**: a. affecting **your computer systems** has not yet been discovered; and b. is still reasonably suspected and/or is a credible threat to **your computer systems**; a continuation of such **voluntary shutdown** may be agreed to, but only with **our** prior written consent, which will not be unreasonably withheld.

emergence

summary of key changes

EXCLUSIONS

POLICY REFERENCE	DESCRIPTION
ALL SECTIONS OF THE POLIICY:	
Exclusion 2	*Modified the write back for mental anguish to ensure employees aren't excluded.* arising from or as a consequence of death or bodily injury, however, this exclusion shall not apply to mental illness caused to individuals, as a result of a **cyber event** and for which **you** are legally liable.
Exclusion 3	*Modified to include additional event triggers of telephone phreaking, cryptojacking, adverse media event, system failure and voluntary shutdown.* arising from any **cyber event**, **telephone phreaking**, **cryptojacking**, **adverse media event**, **system failure**, **multimedia injury**, **voluntary shutdown**, loss, fact, or circumstance known to **your senior management team** or discovered by **your senior management team** before the **policy period**.
Exclusion 7	*Previous Exclusions 7, 8 and 12 have become consolidated into Exclusion 7.* arising from, attributable to, or as a consequence of: c. ionising, radiation or contamination by radioactivity from any nuclear fuel, waste or other hazardous properties of any nuclear assembly or component, d. pollution, and / or e. any electromagnetic field, electromagnetic radiation or electromagnetism
Exclusion 9	*Modified to more closely align to LMA5567A.* arising from: a. directly or indirectly, a **war**, and / or b. a **cyber operation** that is carried out as part of **war**, or the immediate preparation for **war**, and / or c. a **cyber operation** that causes a **state** to become an **impacted state**. Paragraph c. shall not apply to the direct or indirect effect of a **cyber operation** on a **computer system** used by the **policyholder** or its third-party service providers that is not physically located in an **impacted state** but is affected by a **cyber operation**.

emergence

summary of key changes

EXCLUSIONS

POLICY REFERENCE	DESCRIPTION
ALL SECTIONS OF THE POLIICY:	
	Attribution of a cyber operation to a state Notwithstanding **our** burden of proof, which will remain unchanged by this clause, in determining attribution of a **cyber operation** to a **state**, the **policyholder** and **we** will consider such objectively reasonable evidence that is available to them. This may include formal or official attribution by the government of the **state** in which the **computer system** affected by the **cyber operation** is physically located to another **state** or those acting at its direction or under its control.
Exclusion 10	*Modified to address and correct the erroneous write-back with respect to exclusion 9.* caused by or arising out of any **act of terrorism**, however, this exclusion does not apply to the following **cyber events**: **crimeware**, **cyber espionage**, **cyber extortion**, **denial of service**, **hacking**, **payment card skimming**, **point of sale intrusion** or **web app attacks**. This exclusion does however apply to any such activities regardless of whether such activities may also be excluded under Exclusion 9 (war and cyber operation).
Exclusion 11	*Modified to clarify our existing intent that this is a contractual liability exclusion.* for any liability that was assumed by **you** under any contract unless **you** have a liability independent of the contract. This exclusion does not apply to a **payment card industry liability**.
Exclusion 13	*Modified to be more explicit about which infrastructure providers are excluded.* arising out of or attributable to, directly or indirectly, any actual or alleged failure, malfunction or interruption of: a. central securities depositories, central counterparties, trade repositories, security exchanges, clearing houses, or b. a **utility provider**, or c. internet service provider, internet access, internet backbone, or any core infrastructure of the internet (including a failure of the core DNS root servers or the IP address system). This Exclusion will not apply to any of the above which is under **your** direct operational control.

emergence

summary of key changes

EXCLUSIONS

POLICY REFERENCE	DESCRIPTION
ALL SECTIONS OF THE POLIICY:	
Exclusion 21	*Modified to include a write-back for regulatory shutdown to expand Section A.1 – cyber event to your business and Section A.2 – cyber event to your IT contractor's business.* arising from any action of a public or governmental authority, including the expropriation, nationalisation, seizure, confiscation, or destruction of **your computer systems**. This exclusion does not apply to regulatory proceedings, investigations, or civil fines nor does it apply to Section A.1 – cyber event to your business or Section A.2 – cyber event to your IT contractor's business, where there has been a **regulatory shutdown**.
Exclusion 23	*Modified "your computer systems" to "computer systems" to align with the cover under Sections A-D.* caused by defective equipment, ordinary wear or deterioration, faulty design or construction or insufficient capacity of **computer systems**.
Exclusion 25	*Introduction of a theft of money exclusion to clarify existing intent that the policy does not cover financial loss due to theft of money (including digital currency) or securities.* arising from, attributable to, or as a consequence of any financial loss due to the theft of money (including digital currency) or securities.
Exclusion 26	*Introduction of an anti-trust and anti-competition exclusion to clarify existing intent that the policy does not cover such conduct.* arising from or as a consequence of any actual or alleged antitrust violation, restraint of trade, unfair competition, false or unfair trade practices, violation of consumer protection laws or false advertising.
Previous Exclusion 17	*Deleted previous sanctions exclusion and introduced as a general condition (18). Previously endorsed to the policy.*
SECTION B ONLY:	
Exclusion 27	*Exclusion 27 (previously exclusion 28) now applies to D&O liability only. Previously it also applied to liability from providing services to others as an IT contractor. That part of the exclusion is no longer standard.* arising out of, attributable to or in consequence of an action brought against **your** directors or officers acting in that capacity.
Previous exclusion 29	*Previous exclusion 29 excluded liability from providing products or IT services to others for a fee. This has been removed as a standard exclusion.*

emergence

summary of key changes

SECTION I - GENERAL CONDITIONS

POLICY REFERENCE	DESCRIPTION
General Condition 5	*Modified to omit the administrative charge of $110 and the 14-day cooling off period as this policy is not required to have a cooling off period.* **You** may cancel this **policy** at any time by providing **us** with written notice to the email address in **your schedule**, stating when thereafter cancellation is to take effect. As long as no claim has been made and there has been no circumstances that might lead to a **claim**, **cyber event**, **system failure**, **adverse media event**, **voluntary shutdown** or any other incident as covered under this **policy**, we will refund premium to **you** calculated on a pro rata basis less any non-refundable government taxes, charges, or levies. **We** can only cancel the **policy** in accordance with the provisions of the Insurance Contracts Act 1984 (Cth).
General Condition 11	*Modified to replace aggregate with limit, replace preventative shutdown with voluntary shutdown and replace preventative shutdown allowance with voluntary shutdown allowance. We have also modified general condition 11 to address telephone phreaking and introduce data processor response costs and IT contractor response costs.* If you report a **cyber event**, **voluntary shutdown**, **system failure**, **claim**, **multimedia claim**, **adverse media event**, **telephone phreaking** or **cryptojacking** to **us** and either, or all, of **impact on business costs**, **voluntary shutdown allowance**, **loss**, **cyber event response costs**, **reputational harm impact**, **data processor response costs**, **direct financial loss**, **IT contractor response costs** or any other costs as covered under this **policy**, are incurred, then we will apply the **limit** and **excess** set out in **your schedule** as if one such event happened.
General Condition 12	*Modified to replace preventative shutdown with voluntary shutdown, replace aggregate with limit and address telephone phreaking, cryptojacking and Payment Card Industry liability . No change in previous intent.* All reported incidents and claims which arise out of one, or arise out of a series of related, **cyber events**, **voluntary shutdowns Payment Card Industry liabilities**, **system failures**, **telephone phreaking**, **cryptojackings** or **multimedia injuries** involving **your computer systems** or **business** will be deemed to be one **cyber event**, **voluntary shutdown**, **Payment Card Industry liability**, **system failure**, **telephone phreaking**, **cryptojacking** or **multimedia injury** and only one **limit** will apply.

emergence

summary of key changes

SECTION I - GENERAL CONDITIONS

POLICY REFERENCE	DESCRIPTION
General Condition 16	*Modified to elaborate on the dispute resolution process including a mechanism of submitting to a Senior Counsel for determination.* In the event that a dispute arises between **us** and the **policyholder**, or the **policyholder subsidiaries** covered under this **policy**, out of or otherwise in relation to this **policy**, then **we** will, if requested by the **policyholder**, submit the dispute to a Senior Counsel to be mutually agreed or, in default of agreement, the Senior Counsel is to be appointed by the President of the Bar Association in the **policyholder's** resident State or Territory. The Senior Counsel will determine the dispute and issue a determination in writing. The parties agree to share all costs related to the engagement of Senior Counsel equally, with each party responsible for fifty percent (50%). If a dispute does not resolve under the preceding condition, **we**, in accepting this insurance agree that: a. if a dispute arises under this insurance, this **policy** will be subject to Australian law and practice and the **insurers** will submit to the jurisdiction of any competent Court in the Commonwealth of Australia; b. a summons notice or process to be served upon **us** may be served upon: Lloyd's Australia Limited Level 32, 225 George Street Sydney NSW 2000 who has authority to accept, service and to appear on our behalf; c. if a suit is instituted against any of the **insurers**, all the **insurers** participating in this **policy** will abide by the final decision of such Court or any competent Appellate Court.
General Condition 18	*Previous Sanctions Exclusion (17) is now General Condition 18. Previously endorsed to the policy.* **We** will not be deemed to provide cover or 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 **us** 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.