Computer Network Security Liability Extension

Subject to the Definitions, Obligations, Exclusions and General Conditions of the POLICY and any endorsement attached thereto, and the terms of this Extension:

THE INSURER agrees to pay DAMAGES and CLAIM EXPENSES which YOU shall become legally liable to pay because of a COMPUTER NETWORK SECURITY CLAIM first made against YOU during the PERIOD OF INSURANCE and reported to THE INSURER no later than sixty (60) days after the expiration of the PERIOD OF INSURANCE, provided such COMPUTER NETWORK SECURITY CLAIM arises from YOUR (including any person, including an independent contractor, for whose act, error or omission YOU are legally responsible) use of COMPUTER SYSTEMS.

Obligations, Exclusions and General Conditions

1. The coverage provided by this Extension is not applicable to any COMPUTER NETWORK SECURITY CLAIM for which the POLICY otherwise provides coverage.

2. Subject to YOUR obligation to pay the DEDUCTIBLE as is stated in item no. 4 of the CERTIFICATE OF INSURANCE, YOUR LIMIT OF LIABILITY for COMPUTER NETWORK SECURITY CLAIMS covered by this Extension is **$(MANDATORY CLAIM LIMIT APPLICABLE TO THE PRACTICE)** which is the maximum amount payable as DAMAGES by THE INSURER during the PERIOD OF INSURANCE and sixty (60) days following the expiration of the PERIOD OF INSURANCE.

3. THE INSURER will not cover YOU, pay DAMAGES or CLAIM EXPENSES where, with regard to COMPUTER SYSTEMS:

    a) YOU fail to install critical security, anti-virus and malware patches received from commercial software vendors onto all of the COMPUTER SYSTEMS under YOUR control within 14 days of receipt; or

    b) YOU fail to enable and maintain the following security best-practice on YOUR networked COMPUTER SYSTEMS:
        1) filtering of all incoming emails and communications for malicious links, spam, malware and attachments;
        2) Multi-Factor Authentication for all user accounts;
        3) a Sender Policy Framework;
        4) Advanced Threat Protection settings; or

    c) YOU fail to implement a reasonable program of internal network computer security for YOUR employees or others authorised to have access to YOUR COMPUTER SYSTEMS; or

    d) YOU fail to have the following protocols in place:
        1) all system configuration and data on COMPUTER SYSTEMS is either (i) subject to regular back-ups (at least weekly) via secure cloud or (ii) maintained in offline copies disconnected from the organisation's network
        2) Multi-Factor Authentication settings are enabled for access to back-up files
        3) Data is encrypted which it is in transit, at rest and on portable devices.

4. Notwithstanding anything in the POLICY to the contrary, should YOU maintain other insurance covering COMPUTER NETWORK SECURITY CLAIMS, then the coverage afforded under this Extension will apply only as excess and in no event as contributing insurance, and then only after all other insurance has been exhausted, whether or not such insurance is collectible.

5. This Extension excludes any actual or alleged loss, DAMAGES, liability, claim, fine, penalty, cost (including, but not limited to CLAIM EXPENSE) or expense of whatsoever nature directly or indirectly caused by,

contributed to by, resulting from, arising out of or in connection with a PROFESSIONAL SERVICES WRONGFUL ACT

Definitions Applicable to this Extension

1. "COMPUTER NETWORK SECURITY CLAIM" is a CLAIM not otherwise insured by the POLICY or endorsements attached thereto, which results in:

    a. the inability of a third party, who is authorized to do so, to gain access to COMPUTER SYSTEMS; or

    b. the failure to prevent UNAUTHORISED ACCESS to COMPUTER SYSTEMS that results in:
        i. the destruction, deletion or corruption of electronic data on COMPUTER SYSTEMS; or

        ii. THEFT OF DATA from COMPUTER SYSTEMS; or

        iii. denial of service attacks against Internet sites or computers; or

    c. the failure to prevent transmission of MALICIOUS CODE from COMPUTER SYSTEMS to third party computers and systems.

2. "COMPUTER SYSTEMS" means computers and associated input and output devices, data storage devices, networking equipment, and back up facilities:

    i. operated by and either owned by or leased to the NAMED INSURED; or

    ii. operated by a third party service provider and used for the purpose of providing hosted computer application services to the NAMED INSURED or for processing, maintaining, hosting or storing the NAMED INSURED's electronic data, pursuant to written contract with the NAMED INSURED for such services.

3. "MALICIOUS CODE" means any virus, Trojan Horse, worm or other similar software program, code or script intentionally designed to insert itself into computer memory or onto a computer disk and spread itself from one computer to another.

4. "PROFESSIONAL SERVICES WRONGFUL ACT" means any actual or alleged act, error or omission by YOU in the rendering or failure to render professional services to others in YOUR capacity as an architect, engineer, project manager, property consultant, project co-ordinator or surveyor or other professional as otherwise defined in the POLICY to which this Extension is attached.

5. "THEFT OF DATA" means the unauthorized taking, misuse or disclosure of information on COMPUTER SYSTEMS, including but not limited to charge, debit, credit card information, banking, financial, and investment services account information, proprietary information, and personal, private, and confidential information.

6. "UNAUTHORISED ACCESS" means:

    i. the use of or access to COMPUTER SYSTEMS by a person not authorised to do so by the NAMED INSURED; or

    ii. the authorised use of or access to COMPUTER SYSTEMS in a manner not authorised by the NAMED INSURED.

ALL OTHER DEFINITIONS, OBLIGATIONS, PROVISOS, EXCLUSIONS AND GENERAL CONDITIONS OF THE POLICY REMAIN UNCHANGED.