THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

Endorsement No. <Numeric>

Effective Date of this Endorsement: <mm dd, yyyy> **Policy No.** <Alpha Numeric>

EXCLUSION – CYBER PRIVACY EVENT, CYBER SECURITY EVENT, DATA-RELATED LIABILITY, AND INTERRUPTION OR FAILURE OF SERVICES

This endorsement modifies insurance provided under the following:

EXCESS LIABILITY POLICY
EXCESS AUTO LIABILITY POLICY

1. This policy is amended by the addition of the following exclusions which supersede any other provision to the contrary:

   This policy does not apply to:

   Ultimate net loss, loss, **costs** or expenses arising directly or indirectly out of, resulting from, caused by or contributed to by:

   a. Any **cyber privacy event**;

   b. Any **cyber security event**; or

   c. The loss of, loss of use of, damage to, corruption of, inability to access, inability to manipulate, impairment of, or error in the design or manufacture of **electronic data.**

   These exclusions apply even if **ultimate net loss** are claimed for notification costs, credit monitoring expenses, issuance or reissuance of payment cards, attorneys' fees, forensic expenses, public relations expenses or any other loss, cost or expense incurred by any insured or others arising out of that which is described in Paragraph a., b. or c. above, as defined.

   d. Interruption Or Failure Of Services

      (1) Any electrical, telecommunication (including internet service providers), satellite or mechanical failure of infrastructure or service (of any kind or degree whatsoever including, but not limited to, the interruption of electric power supply, power surge, brownouts, blackouts, short circuits, overvoltage, induction or power fluctuation) not under the operational control of the insured;

      (2) Any cessation or slowdown of those activities conducted by **you** in the normal conduct of **your** business or **your** suspension of **your** business activities:

         (a) For the purpose of avoiding or mitigating the possibility of transmitting any malware to another person or entity;

         (b) Due to insufficient capacity to process transactions; or

         (c) Due to an overload of activity on any **information system**.

© General Star Management Company, Stamford, CT 2022
Includes copyrighted material of Insurance Services Office, Inc. with its permission.

SPECIMEN

2. For the purposes of this exclusion, the following definitions apply**:**

   a. **Cyber privacy event** means any actual, alleged, or attempted:

      (1) Access to or disclosure of **protected information;**

      (2) Loss of **protected information;**

      (3) Failure to maintain or provide **your** publicly available privacy policy in compliance with any **privacy or security regulation;** or

      (4) Violation of any **privacy or security regulation.**

   b. **Cyber security event** means any actual, alleged, attempted or threatened:

      (1) Unauthorized access to or unauthorized use of any **information system;**

      (2) Denial of service attack;

      (3) **Social engineering incident;**

      (4) Extortion or ransomware incident;

      (5) Release, introduction, transmission or facilitation of any malware into any **information system;**

      (6) Loss in any way involving cryptocurrency or any other fungible token, non-fungible token (NFT), or any account, wallet, address, or access credential that secure any of the foregoing;

      (7) Loss in any way involving virtual reality, augmented reality or the metaverse; or

      (8) Violation of any **privacy or security regulation.**

   c. **Electronic data** means information, facts or programs stored as or on, created or used on, or transmitted to or from any **information system.**

   d. **Information system** means any:

      (1) Electronic hardware including, but not limited to, any:

         (a) Computer;

         (b) Transportable, mobile or handheld device;

         (c) Operational Technology (OT) or Industrial Control System (ICS) machinery, equipment or device (including but not limited to Industrial Internet of Things (IIoT) machinery, equipment or device);

         (d) Internet of Things (IoT) device;

         (e) Network equipment;

         (f) Electronic data storage (including but not limited to any hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices, any other media, storage area network (SAN) or electronic data backup facility);

         (g) Associated input and output device; or

         (h) Related component;

      (2) Paper storage;

      (3) Software (including but not limited to firmware, middleware, software components, operating systems, client-server based software, individual applications, network related software, artificial intelligence, or any other software that is distinct from any of the foregoing);

      (4) Communication network (including but not limited to those used in connection with the items described in paragraphs d.(1) through d.(3) above; or

      (5) Interface or other means (including but not limited to those items described in paragraphs d.(1) through d.(4) above) by which any user interacts with any computer system.

SPECIMEN

© General Star Management Company, Stamford, CT 2022
Includes copyrighted material of Insurance Services Office, Inc. with its permission.

Paragraphs d.(1) through paragraphs d.(5) above include, but are not limited to, any software-as-a-service (SaaS), platform-as-a-service (PaaS), web/cloud or other multi-tenant service or storage model.

e. **Privacy or security regulation** means any federal, state, local or foreign current or future statute, law, rule or regulation associated with the control, correction, collection, protection, retention, handling, disposal, processing, disclosure, sharing, sale, maintenance, acquisition, storage, access to, use or misuse, of **protected information**.

Privacy or security regulation includes but is not limited to:

(1) The Health Insurance Portability and Accountability Act of 1996 (as amended) (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and their implementing regulations, or protected health-related information under any similar federal, state, local or foreign law;

(2) The Gramm-Leach Bliley Act of 1999 and its implementing regulations;

(3) The California Security Breach Notification Act (CA SB 1386) and Massachusetts 201 CMR 17.00;

(4) The Identity Theft Red Flags under the Fair and Accurate Credit Transactions Act of 2003;

(5) The Fair Credit Reporting Act (15. U.S.C. §1681);

(6) Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. §45(a), but solely for alleged violations of unfair or deceptive acts or practices in or affecting commerce;

(7) The Data Protection Act of 1998 or similar legislation to comply with the European Union Data Protection Directive 95/45/EC of 1995;

(8) The European Union General Data Protection Regulation (Regulation (EU) 2016/679 – GDPR);

(9) The New York Cybersecurity Regulation (23 NYCRR Part 500);

(10) The California Consumer Privacy Act of 2018;

(11) The California Privacy Rights Act of 2020:

(12) The Biometric Information Privacy Act (740 ILCS 14/); or

(13) Any other federal, state, local or foreign statute, law, rule or regulation concerning data protection or information security.

f. **Protected information** means any:

(1) Information not available to the general public through which an individual may be identified, as set forth in any **privacy or security regulation,** including (but not limited to) an individual's:

(a) Social security number, driver's license number or state identification number;

(b) Protected health information;

(c) Financial account numbers;

(d) Security codes, passwords, personal identification numbers associated with credit, debit or charge card numbers which would permit access to financial accounts;

(e) Biometric data; or

(f) Any other nonpublic information as set forth in any **privacy or security regulation;** or

(2) Business records, customer lists, intellectual property (including but not limited to patents, trade secrets, data, designs, interpretations, forecasts, methods, practices, processes, reports, ideas or expressions of ideas) or any other non-public information entrusted to an insured under a written contract to protect its confidentiality.

SPECIMEN

© General Star Management Company, Stamford, CT 2022
Includes copyrighted material of Insurance Services Office, Inc. with its permission.

g. **Social engineering incident** means any insured:

(1) Having transferred, paid or delivered funds, data or information; or

(2) Accepted, completed or relayed instructions

as a result of any deceptive, misleading or deceitful instruction (including but not limited to any written, electronic, virtual, telephone or in-person instruction).

ALL OTHER TERMS AND CONDITIONS OF THIS POLICY REMAIN UNCHANGED.

SPECIMEN

© General Star Management Company, Stamford, CT 2022
Includes copyrighted material of Insurance Services Office, Inc. with its permission.