ENDORSEMENT NO.

NEW YORK CYBER SUITE COVERAGE ENDORSEMENT

This Endorsement, effective at 12:01 a.m. on , forms part of

Policy No.
Issued to
Issued by: The Hartford Steam Boiler Inspection and Insurance Company

This endorsement modifies insurance provided under the following:

Social Worker Professional and Business Liability Policy

PLEASE NOTE THAT DEFENSE COSTS ARE CONTAINED WITHIN THE THIRD PARTY LIMIT OF LIABILITY AND SUBJECT TO THE DEDUCTIBLE. THIS MEANS THAT THE THIRD PARTY LIMIT OF LIABILITY SPECIFIED IN THIS CYBER SUITE COVERAGE SHALL BE REDUCED, AND MAY BE COMPLETELY EXHAUSTED, BY DEFENSE COSTS. IN THE EVENT THAT THE THIRD PARTY LIMIT OF LIABILITY IS EXHAUSTED, THE INSURER SHALL NOT BE LIABLE FOR FURTHER DEFENSE COSTS OR FOR ANY DAMAGES OR JUDGMENTS. THIS CYBER SUITE COVERAGE IS COMPRISED OF FIRST PARTY AND THIRD PARTY COVERAGES. THE FIRST PARTY COVERAGE PROVIDED BY THIS ENDORSEMENT IS WRITTEN ON A DISCOVERY BASIS. THE THIRD PARTY COVERAGE PROVIDED BY THIS ENDORSEMENT IS WRITTEN ON A CLAIMS-MADE BASIS AND PROVIDES NO COVERAGE FOR CLAIMS ARISING OUT OF INCIDENTS, OCCURRENCES OR ALLEGED WRONGFUL ACTS WHICH TOOK PLACE PRIOR TO THE FIRST INCEPTION OF THIS CYBER SUITE COVERAGE. THIS THIRD PARTY COVERAGE COVERS ONLY CLAIMS ACTUALLY MADE AGAINST THE INSURED WHILE THE COVERAGE REMAINS IN EFFECT, AND ALL THIRD PARTY COVERAGE UNDER THIS ENDORSEMENT CEASES UPON THE TERMINATION OF THE COVERAGE, EXCEPT FOR THE AUTOMATIC EXTENDED REPORTING PERIOD COVERAGE, UNLESS THE INSURED PURCHASES ADDITIONAL EXTENDED REPORTING PERIOD COVERAGE. THIS THIRD PARTY COVERAGE PROVIDES AN AUTOMATIC EXTENDED REPORTING PERIOD OF 60 DAYS. A

SUPPLEMENTAL EXTENDED REPORTING PERIOD OF 1 YEAR MAY BE PURCHASED BY YOU FOR AN ADDITIONAL PREMIUM OF 98% OF THE FULL ANNUAL PREMIUM APPLICABLE TO THE THIRD PARTY COVERAGE OF THIS CYBER SUITE COVERAGE. BECAUSE THE EXTENDED REPORTING PERIOD IS NOT UNLIMITED, POTENTIAL COVERAGE GAPS MAY ARISE UPON ITS EXPIRATION. AS THE THIRD PARTY COVERAGE PROVIDED BY THIS CYBER SUITE COVERAGE IS WRITTEN ON A CLAIMS-MADE BASIS, THIRD PARTY COVERAGE RATES ARE LOWER IN THE EARLIER YEARS THAN FOR AN OCCURRENCE POLICY, AND YOU SHOULD EXPECT SUBSTANTIAL ANNUAL PREMIUM INCREASES, INDEPENDENT OF OVERALL RATE INCREASES, UNTIL THE CLAIMS-MADE RELATIONSHIP REACHES MATURITY.

Throughout this Coverage Endorsement (hereinafter referred to as "Cyber Coverage"), the words "you" and "your" refer to the Named Insured(s) shown in the Cyber Suite Supplemental Declarations of this Cyber Coverage and any other person(s) or organization(s) qualifying as a Named Insured under this Cyber Coverage. The words "we", "us" and "our" refer to the company providing this insurance.

Other words and phrases that appear in quotations have special meaning, specifically applicable to this endorsement. Refer to **DEFINITIONS**. Any definitions contained in any other coverage provided under this policy do not apply to this endorsement, unless specifically stated otherwise in an endorsement(s) attached hereto.

The terms and conditions of Section **X. CANCELLATION** or Section **XI. CANCELLATION**, as applicable, and any amendment to such terms incorporated by endorsement are hereby incorporated herein and shall apply to coverage as is afforded by this Cyber Coverage, unless specifically stated otherwise in an endorsement(s) attached hereto.

A. COVERAGE

This section lists the coverages that apply only if indicated in the Cyber Suite Supplemental Declarations.

1. Data Compromise Response Expenses

a. Data Compromise Response Expenses applies only if all of the following conditions are met:

(1) There has been a "personal data compromise"; and

(2) Such "personal data compromise" took place in the "coverage territory"; and

(3) Such "personal data compromise" is first discovered by you during the "policy period"; and

(4) Such "personal data compromise" is reported to us as soon as practicable after the date it is first discovered by you.

b. If the conditions listed in **a.** above have been met, then we will provide coverage for the following expenses when they arise directly from such "personal data compromise" and are necessary and reasonable. Items **(4)** and **(5)** below apply only if there has been a notification of the "personal data compromise" to "affected individuals" as covered under item **(3)** below.

(1) Forensic IT Review

We will pay for a professional information technologies review if needed to determine, within the constraints of what is possible and reasonable, the nature and extent of the "personal data compromise" and the number and identities of the "affected individuals".

This does not include costs to analyze, research or determine any of the following:

(a) Vulnerabilities in systems, procedures or physical security;

(b) Compliance with Payment Card Industry or other industry security standards; or

(c) The nature or extent of "loss" or damage to data that is not "personally identifying information" or "personally sensitive information".

If there is reasonable cause to suspect that a covered "personal data compromise" may have occurred, we will pay for costs covered under Forensic IT Review, even if it is eventually determined that there was no covered "personal data compromise". However, once it is determined that there was no covered "personal data compromise", we will not pay for any further costs.

(2) Legal Review

We will pay for a professional legal counsel review of the "personal data compromise" and how you should best respond to it.

If there is reasonable cause to suspect that a covered "personal data compromise" may have occurred, we will pay for costs covered under Legal Review, even if it is eventually determined that there was no covered "personal data compromise". However, once it is determined that there was no covered "personal data compromise", we will not pay for any further costs.

(3) Notification to Affected Individuals

We will pay your necessary and reasonable costs to provide notification of the "personal data compromise" to "affected individuals".

(4) Services to Affected Individuals

We will pay your necessary and reasonable costs to provide the following services to "affected individuals". Services **(c)** and **(d)** below apply only to "affected individuals" from "personal data compromise" events involving "personally identifying information".

(a) Informational Materials

A packet of loss prevention and customer support information.

(b) Help Line

A toll-free telephone line for "affected individuals" with questions about the "personal data compromise". Where applicable, the line can also be used to request additional services as listed in **(c)** and **(d)** below.

(c) Credit Report and Monitoring

A credit report and an electronic service automatically monitoring for activities affecting an individual's credit records. This service is subject to the "affected individual" enrolling for this service with the designated service provider.

(d) Identity Restoration Case Management

As respects any "affected individual" who is or appears to be a victim of "identity theft" that may reasonably have arisen from the "personal data compromise", the services of an identity restoration professional who will assist that "affected individual" through the process of correcting credit and other records and, within the constraints of what is possible and reasonable, restoring control over his or her personal identity.

You may select a provider for any of the services described in this section **b.** in accordance with the parameters provided under **11. Service Providers**.

(5) Public Relations

We will pay for a professional public relations firm review of, and response to, the potential impact of the "personal data compromise" on your business relationships.

This includes necessary and reasonable costs to implement public relations recommendations of such firm. This may include advertising and special promotions designed to retain your relationship with "affected individuals". However, we will not pay for:

(a) Promotions provided to any of your directors or employees; or

(b) Promotion costs exceeding $25 per "affected individual".

2. Computer Attack

a. Computer Attack applies only if all of the following conditions are met:

(1) There has been a "computer attack"; and

(2) Such "computer attack" occurred in the "coverage territory"; and

(3) Such "computer attack" is first discovered by you during the "policy period"; and

(4) Such "computer attack" is reported to us as soon as practicable after the date it is first discovered by you.

b. If the conditions listed in **a.** above have been met, then we will provide you the following coverages for "loss" directly arising from such "computer attack".

(1) Data Restoration

We will pay your necessary and reasonable "data restoration costs".

(2) Data Re-creation

We will pay your necessary and reasonable "data re-creation costs".

(3) System Restoration

We will pay your necessary and reasonable "system restoration costs".

(4) Loss of Business

We will pay your actual "business income and extra expense loss" incurred during the "period of restoration".

(5) Public Relations

If you suffer a covered "business income and extra expense loss", we will pay for the services of a professional public relations firm to assist you in communicating your response to the "computer attack" to the media, the public and your customers, clients or members.

3. Cyber Extortion

a. Cyber Extortion applies only if all of the following conditions are met:

(1) There has been a "cyber extortion threat"; and

(2) Such "cyber extortion threat" is first made against you during the "policy period"; and

(3) Such "cyber extortion threat" is reported to us as soon as practicable after the date it is first made against you.

b. If the conditions listed in **a.** above have been met, then we will pay for your necessary and reasonable "cyber extortion expenses" arising directly from such "cyber extortion threat". The payment of "cyber extortion expenses" must be approved in advance by us. We will not pay for "cyber extortion expenses" that have not been approved in advance by us. We will not unreasonably withhold approval.

c. You must make every reasonable effort not to divulge the existence of this Cyber Extortion coverage.

4. Data Compromise Liability

a. Data Compromise Liability applies only if all of the following conditions are met:

(1) During the "policy period" or any applicable Extended Reporting Period, you first receive notice of one of the following:

(a) A "claim" brought by or on behalf of one or more "affected individuals"; or

(b) A "regulatory proceeding" brought by a government entity.

(2) Such "claim" or "regulatory proceeding" must arise from a "personal data compromise" that:

(a) Took place during the "coverage term"; and

(b) Took place in the "coverage territory".

(3) Such "claim" or "regulatory proceeding" is reported to us as soon as practicable, after the date it is first received by you.

b. If the conditions listed in **a.** above have been met, then we will pay on your behalf any covered:

(1) "Loss" directly arising from the "claim"; or

(2) "Defense costs" directly arising from a "regulatory proceeding".

c. All "claims" and "regulatory proceedings" arising from a single "personal data compromise" or interrelated "personal data compromises" will be deemed to have been made at the time that notice of the first of those "claims" or "regulatory proceedings" is received by you.

B. EXCLUSIONS

The following additional exclusions apply to the coverage provided by this endorsement:

We will not pay for costs or "loss" arising from, based upon, or alleging the following:

1. War and military action including any of the following and any consequence of any of the following:

a. War, including undeclared or civil war;

b. Warlike action by military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or

c. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these.

2. Failure or interruption of, or damage to, any electrical power supply network or telecommunications network not owned and operated by you including, but not limited to, the internet, internet service providers, Domain Name System (DNS) service providers, cable and wireless providers, internet exchange providers, search engine providers, internet protocol networks (and similar networks that may have different designations) and other providers of telecommunications or internet infrastructure.

3. Any attack on, incident involving, or loss to any computer or system of computers that is not a "computer system".

4. Costs to research or correct any deficiency.

5. Any fines or penalties.

6. Any criminal investigations or proceedings.

7. Your intentional or willful complicity in a covered "loss" event.

8. Your reckless disregard for the security of your "computer system" or data, including confidential or sensitive information of others in your care, custody or control.

9. Any criminal, fraudulent, malicious or dishonest act, error or omission, or any intentional or knowing violation of any statute, rule or law by you.

10. Any "personal data compromise", "computer attack" or "cyber extortion threat" discovered before

the "policy period".

11. Any "wrongful act" occurring before the "coverage term".

12. That part of any "claim" seeking any non-monetary relief. However, this exclusion does not apply to "defense costs" arising from an otherwise insured "wrongful act".

13. The propagation or forwarding of malware, including viruses, worms, Trojans, spyware and key loggers in connection with hardware or software created, produced or modified by you for sale, lease or license to third parties.

14. "Property damage" or "bodily injury".

15. Under any Liability Coverage, to "loss" or "claim":

a. With respect to which an insured under the policy is also an insured under a nuclear energy liability policy issued by Nuclear Energy Liability Insurance Association, Mutual Atomic Energy Liability Underwriters, Nuclear Insurance Association of Canada or any of their successors, or would be an insured under any such policy but for its termination upon exhaustion of its limit of liability; or

b. Resulting from the "hazardous properties" of "nuclear material" and with respect to which (a) any person or organization is required to maintain financial protection pursuant to the Atomic Energy Act of 1954, or any law amendatory thereof, or (b) the insured is, or had this policy not been issued would be, entitled to indemnity from the United States of America, or any agency thereof, under any agreement entered into by the United States of America, or any agency thereof, with any person or organization.

16. Under any Liability Coverage, to "loss" or "claim" resulting from "hazardous properties" of "nuclear material", if:

a. The "nuclear material" **(a)** is at any "nuclear facility" owned by, or operated by or on behalf of, an insured or **(b)** has been discharged or dispersed therefrom;

b. The "nuclear material" is contained in "spent fuel" or "waste" at any time possessed, handled, used, processed, stored, transported or disposed of, by or on behalf of an insured; or

c. The "loss" or "claim" arises out of the furnishing by an insured of services, materials, parts or equipment in connection with planning, construction, maintenance, operation or use of any "nuclear facility", but if such facility is located within the United States of America, its territories or possessions or Canada, this exclusion **c.** applies only to "property damage" to such "nuclear facility" and any property threat.

The following definitions apply exclusively to Exclusions **15.** & **16.**:

"Hazardous properties" includes radioactive, toxic or explosive properties.

"Nuclear material" means "source material", "special nuclear material" or "by-product material".

"Source material", "special nuclear material" and "by-product material" have the meanings given them in the Atomic Energy Act of 1954 or in any law amendatory thereof.

"Spent fuel" means any fuel element or fuel component, solid or liquid, which has been used or exposed to radiation in a "nuclear reactor".

"Waste" means any waste material **(a)** containing "by-product material" other than the tailing or wastes produced by the extraction or concentration of uranium or thorium from any ore processed primarily for its "source material" content, and **(b)** resulting from the operation by any person or organization of any "nuclear facility" included under the first two paragraphs of the definition of "nuclear facility".

"Nuclear facility" means:

(a) Any "nuclear reactor";

(b) Any equipment or device designed or used for **(1)** separating the isotopes of uranium or plutonium, **(2)** processing or utilizing "spent fuel", or **(3)** handling, processing or packaging "waste";

(c) Any equipment or device used for the processing, fabricating or alloying of 'special nuclear material" if at any time the total amount of such material in the custody of the insured at the premises where such equipment or device is located consists of or contains more than 25 grams of

plutonium or uranium 233 or any combination thereof, or more than 250 grams of uranium 235;

(d) Any structure, basin, excavation, premises or place prepared or used for the storage or disposal of "waste";

And includes the site on which any of the foregoing is located, all operations conducted on such site and all premises used for such operations.

"Nuclear reactor" means any apparatus designed or used to sustain nuclear fission in a self-supporting chain reaction or to contain a critical mass of fissionable material.

"Property damage" includes all forms of radioactive contamination of property.

C. LIMITS OF INSURANCE

1. Aggregate Limits

The First Party Annual Aggregate Limit shown in the Cyber Suite Supplemental Declarations is the most we will pay for all "loss" under all the Data Compromise Response Expenses, Computer Attack or Cyber Extortion coverages in any one "policy period". The First Party Annual Aggregate Limit shown in the Cyber Suite Supplemental Declarations applies regardless of the number of insured events first discovered during the "policy period".

Except for post-judgment interest, the Third Party Annual Aggregate Limit shown in the Cyber Suite Supplemental Declarations is the most we will pay for all "loss" under all the Data Compromise Liability coverage in any one "policy period" or any applicable Extended Reporting Period. The Third Party Annual Aggregate Limit shown in the Cyber Suite Supplemental Declarations applies regardless of the number of insured "claims" or "regulatory proceedings" first received during the "policy period" or any applicable Extended Reporting Period.

2. Coverage Sublimits

a. Data Compromise Sublimits

The most we will pay under Data Compromise Response Expenses for Forensic IT Review, Legal Review and Public Relations coverages for "loss" arising from any one "personal data compromise" is the applicable sublimit for each of those coverages shown in the Cyber Suite Supplemental Declarations.

These sublimits are part of, and not in addition to, the First Party Annual Aggregate Limit shown in the Cyber Suite Supplemental Declarations. Public Relations coverage is also subject to a limit per "affected individual" as described in **A.1.b.(5)**.

b. Computer Attack Sublimits

The most we will pay under Computer Attack for Loss of Business and Public Relations coverages for "loss" arising from any one "computer attack" is the applicable sublimit for each of those coverages shown in the Cyber Suite Supplemental Declarations. These sublimits are part of, and not in addition to, the First Party Aggregate Limit shown in the Cyber Suite Supplemental Declarations.

c. Cyber Extortion Sublimit

The most we will pay under Cyber Extortion coverage for "loss" arising from one "cyber extortion threat" is the applicable sublimit shown in the Cyber Suite Supplemental Declarations. This sublimit is part of, and not in addition to, the First Party Annual Aggregate Limit shown in the Cyber Suite Supplemental Declarations.

3. Application of Limits

a. A "computer attack", "cyber extortion threat" or "personal data compromise" may be first discovered by you in one "policy period" but it may cause insured "loss" in one or more subsequent "policy periods". If so, all insured "loss" arising from such "computer attack", "cyber extortion threat" or "personal data compromise" will be subject to the limit of insurance applicable to the "policy period" when the "computer attack", "cyber extortion threat" or "personal data compromise" was first discovered by you.

b. You may first receive notice of a "claim" or "regulatory proceeding" in one "policy period" but it may cause insured "loss" in one or more subsequent "policy periods". If so, all insured

"loss" arising from such "claim" or "regulatory proceeding" will be subject to the limit of insurance applicable to the "policy period" when notice of the "claim" or "regulatory proceeding" was first received by you. The applicable limit of insurance is a per occurrence limit applicable to a single "claim" or "regulatory proceeding". The insured loss is also subject to an annual aggregate limit.

c. The limit of insurance for the Extended Reporting Periods (if applicable) will be part of, and not in addition to, the limit of insurance for the immediately preceding "policy period".

d. Coverage for Services to Affected Individuals under Data Compromise Response Expenses is limited to costs to provide such services for a period of up to one year from the date of the notification to the "affected individuals". Notwithstanding, coverage for Identity Restoration Case Management services initiated within such one year period may continue for a period of up to one year from the date such Identity Restoration Case Management services are initiated.

D. DEDUCTIBLES

1. We will not pay for "loss" until the amount of the insured "loss" exceeds the deductible amount shown in the Cyber Suite Supplemental Declarations. We will then pay the amount of "loss" in excess of the applicable deductible amount, subject to the applicable limits shown in the Cyber Suite Supplemental Declarations. You will be responsible for the applicable deductible amount.

We may pay any part or all of the deductible to effect settlement of a "loss" and upon notification of the action taken, you shall promptly reimburse us for such part or all of the deductible as we may have paid.

2. The deductible will apply to all:

a. "Loss" arising from the same insured event or interrelated insured events under Data Compromise Response Expenses, Computer Attack or Cyber Extortion.

b. "Loss" resulting from the same "wrongful act" or interrelated "wrongful acts" insured under Data Compromise Liability.

3. In the event that "loss" is insured under more than one coverage section, only the single highest deductible applies.

E. ADDITIONAL CONDITIONS

The following conditions apply:

1. Bankruptcy

Your bankruptcy or insolvency, or if you are a sole proprietor, the insolvency of your estate, will not release us from the payment of damages for injury sustained or loss occasioned during the life of and within the coverage of this Cyber Coverage.

2. Defense And Settlement

a. We shall have the right and the duty to assume the defense of any applicable "claim" or "regulatory proceeding" against you even if the allegations in the "claim" are groundless, false or fraudulent. You shall give us such information and cooperation as we may reasonably require.

b. You shall not admit liability for or settle any "claim" or "regulatory proceeding" or incur any defense costs without our prior written consent.

c. If you refuse to consent to any settlement recommended by us and acceptable to the claimant, we may then withdraw from your defense by tendering control of the defense to you. From that point forward, you shall, at your own expense, negotiate or defend such "claim" or "regulatory proceeding" independently of us. Our liability shall not exceed the amount for which the "claim" or suit could have been settled if such recommendation was consented to, plus "defense costs" incurred by us, and "defense costs" incurred by you with our written consent, prior to the date of such refusal.

d. We will not be obligated to pay any "loss" or "defense costs", or to defend or continue to defend any "claim" or "regulatory proceeding" after the applicable limit of insurance has been exhausted.

e. We will pay all interest on that amount of any judgment within the applicable limit of insurance which accrues:

(1) After entry of judgment; and

(2) Before we pay, offer to pay or deposit in court that part of the judgment within the applicable limit of insurance or, in any case, before we pay or offer to pay the entire applicable limit of insurance.

These interest payments will be in addition to and not part of the applicable limit of insurance.

f. You shall have the option to: **(1)** select a defense attorney or consent to our choice of defense attorney, which consent shall not be unreasonably withheld; **(2)** participate in and assist in the direction of the defense of any "claim" or "regulatory proceeding"; and **(3)** consent to a settlement, which consent shall not be unreasonably withheld.

g. We shall, upon your written request, provide an accounting of "defense costs" actually expended.

h. Transfer of Control

(1) If we conclude that, based on "claims" or "regulatory proceedings" which have been reported to us and to which this insurance may apply, the applicable limit is likely to be used up in the payment of judgments, "settlement costs", or "defense costs", we will notify you in writing to that effect.

(2) When the applicable limit has actually been used up in the payment of judgments, "settlement costs" or "defense costs":

(a) We will notify you in writing, as soon as practicable, that:

(i) Such applicable limit has actually been used up; and

(ii) Our duty to defend "claims" or "regulatory proceedings" seeking damages subject to the applicable limit has also ended.

(b) We will initiate, and cooperate in, the transfer of control to you, of all "claims" and "regulatory proceedings" seeking damages which are subject to the applicable limit and which are reported to us before the applicable limit is used up. You must cooperate in the transfer of control of said "claims" and "regulatory proceedings".

We agree to take such steps, as we deem appropriate, to avoid a default in, or continue the defense of, such "claims" and "regulatory proceedings" until such transfer is completed, provided you are cooperating in completing such transfer.

We will take no action whatsoever with respect to any "claim" or "regulatory proceeding" seeking damages that would have been subject to the applicable limit, had it not been used up, if the "claim" or "regulatory proceeding" is reported to us after the applicable limit has been used up.

(c) You must arrange for the defense of such "claims" or "regulatory proceedings" within such time period as agreed to between you and us. Absent any such agreement, arrangements for the defense of such "claims" or "regulatory proceedings" must be made as soon as practicable.

i. In applying the foregoing, in the event incidental coverage for legal services is provided under this Cyber Suite coverage, such coverage shall be provided in accordance with Part 71.3 of 11 NYCRR 107 as amended, and shall not reduce the per claim or aggregate limits of liability greater than 25 percent.

3. Due Diligence

You agree to use due diligence to prevent and mitigate "loss" insured under this Cyber Coverage. This includes, but is not limited to, complying with, and requiring your vendors to comply with, reasonable and industry-accepted protocols for:

a. Providing and maintaining appropriate physical security for your premises, "computer systems" and hard copy files;

b. Providing and maintaining appropriate computer and Internet security;

c. Maintaining and updating at appropriate intervals backups of computer data;

d. Protecting transactions, such as processing credit card, debit card and check payments; and

e. Appropriate disposal of files containing "personally identifying information", "personally sensitive information" or "third party corporate data", including shredding hard copy files and destroying physical media used to store electronic data.

4. Duties in the Event of a Claim, Regulatory Proceeding or Loss

a. If, during the "policy period", incidents or events occur which you reasonably believe may give rise to a "claim" or "regulatory proceeding" for which coverage may be provided hereunder, such belief being based upon either written notice from the potential claimant or the potential claimant's representative; or notice of a complaint filed with a federal, state or local agency; or upon an oral "claim", allegation or threat, you shall give written notice to us as soon as practicable.

b. If a "claim" or "regulatory proceeding" is brought against you, you must:

(1) Immediately record the specifics of the "claim" or "regulatory proceeding" and the date received;

(2) Provide us with written notice, as soon as reasonably practicable after the date the "claim" or "regulatory proceeding" is first received by you. Written notice given by you or on your behalf, or written notice by or on behalf of the injured person or any other claimant, to any of our licensed agents in this state with particulars sufficient to identify you, shall be deemed notice to us;

(3) Immediately send us copies of any demands, notices, summonses or legal papers received in connection with the "claim" or "regulatory proceeding";

(4) Authorize us to obtain records and other information;

(5) Cooperate with us in the investigation, settlement or defense of the "claim" or "regulatory proceeding";

(6) Assist us, upon our request, in the enforcement of any right against any person or organization which may be liable to you because of "loss" or "defense costs" to which this insurance may also apply; and

(7) Not take any action, or fail to take any required action, that prejudices your rights or our rights with respect to such "claim" or "regulatory proceeding".

c. In the event of a "personal data compromise", "computer attack" or "cyber extortion threat", insured under this Cyber Coverage, you must see that the following are done:

(1) Notify the police if a law may have been broken.

(2) Notify us as soon as practicable after the "personal data compromise", "computer attack" or "cyber extortion threat". Include a description of any property involved.

(3) As soon as possible, give us a description of how, when and where the "personal data compromise", "computer attack" or "cyber extortion threat" occurred.

(4) As often as may be reasonably required, permit us to:

(a) Inspect the property proving the "personal data compromise", "computer attack" or "cyber extortion threat";

(b) Examine your books, records, electronic media and records and hardware;

(c) Take samples of damaged and undamaged property for inspection, testing and analysis; and

(d) Make copies from your books, records, electronic media and records and hardware.

(5) Send us signed, sworn proof of "loss" containing the information we request to investigate the "personal data compromise", "computer attack" or "cyber extortion threat". You must do this within 60 days after our request. We will supply you with the necessary forms.

(6) Cooperate with us in the investigation or settlement of the "personal data compromise", "computer attack" or "cyber extortion threat".

(7) If you intend to continue your business, you must resume all or part of your operations as quickly as possible.

(8) Make no statement that will assume any obligation or admit any liability, for any "loss" for which we may be liable, without our prior written consent.

(9) As soon as reasonably possible, send us any legal papers or notices received concerning the "loss".

d. We may examine you under oath at such times as may be reasonably required, about any matter relating to this insurance or the "claim", "regulatory proceeding" or "loss", including all your books and records. In the event of an examination, your answers must be signed.

e. You may not, except at your own cost, voluntarily make a payment, assume any obligation, or incur any expense without our prior written consent.

5. Employees and Affiliated People

Any person employed or otherwise affiliated with you and covered under this insurance during such employment or affiliation shall continue to be covered under this insurance, including any extended reporting period, after such employment or affiliation has ceased for such person.

6. Extended Reporting Periods

a. You will have the right to the Extended Reporting Periods described in this section, in the event of a "termination of coverage".

Within 30 days after "termination of coverage" we will advise you in writing of the Automatic Extended Reporting Period coverage and the availability of, the premium for, and the importance of purchasing additional extended reporting period coverage.

b. If a "termination of coverage" has occurred, you will have the right to the following:

(1) At no additional premium, an Automatic Extended Reporting Period of 60 days immediately following the effective date of the "termination of coverage" during which you may first receive notice of a "claim" or "regulatory proceeding" arising directly from a "wrongful act" occurring before the end of the "policy period" and which is otherwise insured by this Cyber Coverage; and

(2) Upon payment of the additional premium of 98% of the full annual premium associated with the relevant coverage based on the rates in effect at the beginning of the "policy period", a Supplemental Extended Reporting Period of one year immediately following the effective date of the "termination of coverage" during which you may first receive notice of a "claim" or "regulatory proceeding" arising directly from a "wrongful act" occurring prior to the "termination of coverage" and which is otherwise insured by this Cyber Coverage.

To obtain the Supplemental Extended Reporting Period, you must request it in writing and pay the additional premium due, before the later of 60 days after the effective date of "termination of coverage" or 30 days after we have advised you in writing of the automatic extended reporting period and the availability of, the premium for, and the importance of purchasing additional extended reporting period coverage. The additional premium for the Supplemental Extended Reporting Period will be fully earned at the inception of the Supplemental Extended Reporting Period. If we do not receive the written request as required, you may not exercise this right at a later date.

This insurance, provided during the Supplemental Extended Reporting Period, is excess over any other valid and collectible insurance that begins or continues in effect after the Supplemental Extended Reporting Period becomes effective, whether the other insurance applies on a primary, excess, contingent, or any other basis.

(3) The Supplemental Extended Reporting Period will be available upon "termination of coverage" if **(i)** you have been placed in liquidation or bankruptcy or permanently cease operations; **(ii)** you or your designated trustee does not purchase extended reporting period

coverage; **(iii)** you or your designated trustee requires the extended reporting period coverage within 120 days of the "termination of coverage". We will charge the person for whom extended reporting period coverage is provided a premium commensurate with such coverage.

7. Failure to Give Notice

The failure to give any notice required to be given by this Cyber Coverage within the time prescribed herein shall not invalidate any claim made by you, an injured person or any other claimant, unless the failure to provide timely notice has prejudiced us. The failure to give any notice required to be given by this endorsement within the time prescribed herein shall not invalidate any claim made by you, an injured person or any other claimant if it shall be shown not to have been reasonably possible to give such notice within the prescribed time and that notice was given as soon as was reasonably possible thereafter.

If the insurer disclaims liability or denies coverage based upon the failure to provide timely notice, then the injured person or other claimant may maintain an action directly against such insurer, in which the sole question is the insurer's disclaimer or denial based on the failure to provide timely notice, unless within sixty days following such disclaimer or denial, you or the insurer: **1)** initiates an action to declare the rights of the parties under the insurance policy; and **2)** names the injured person or other claimant as a party to the action.

8. Legal Action Against Us

No one may bring a legal action against us under this insurance unless:

There has been full compliance with all of the terms of this Cyber Coverage and the amount of your obligation to pay has been finally determined either by:

a. Judgment against you which remains unsatisfied at the expiration of thirty (30) days from the service of notice of entry of the judgment upon you and upon us; or

b. Written agreement of you, the claimant and us.

Any person or organization or legal representative thereof who has secured such judgment or written agreement shall thereafter be entitled to recover under this Cyber Coverage to the extent of the insurance afforded by this Cyber Coverage. We may not be impleaded by you or your legal representative in any legal action brought against you by any person or organization.

9. Legal Advice

We are not your legal advisor. Our determination of what is or is not insured under this Cyber Coverage does not represent advice or counsel from us about what you should or should not do.

10. Pre-Notification Consultation

You agree to consult with us prior to the issuance of notification to "affected individuals". We assume no responsibility under Data Compromise Response Expenses for any services promised to "affected individuals" without our prior agreement. If possible, this pre-notification consultation will also include the designated service provider(s) as agreed to under the Service Providers condition below. You must provide the following at our pre-notification consultation with you:

a. The exact list of "affected individuals" to be notified, including contact information.

b. Information about the "personal data compromise" that may appropriately be communicated with "affected individuals".

c. The scope of services that you desire for the "affected individuals". For example, coverage may be
structured to provide fewer services in order to make those services available to more "affected individuals" without exceeding the available Data Compromise Response Expenses limit of insurance.

11. Service Providers

a. We will only pay under this Cyber Coverage for services that are provided by service providers approved by us. You must obtain our prior approval for any service provider whose expenses you want covered under this Cyber Coverage. We will not unreasonably withhold such

approval.

b. Prior to the Pre-Notification Consultation described in the Pre-Notification Consultation Condition above, you must come to agreement with us regarding the service provider(s) to be used for the Notification to Affected Individuals and Services to Affected Individuals. We will suggest a service provider. If you prefer to use an alternate service provider, our coverage is subject to the following limitations:

(1) Such alternate service provider must be approved by us;

(2) Such alternate service provider must provide services that are reasonably equivalent or superior in both kind and quality to the services that would have been provided by the service provider we had suggested; and

(3) Our payment for services provided by any alternate service provider will not exceed the amount that we would have paid using the service provider we had suggested.

12. Services

The following conditions apply as respects any services provided to you or any "affected individual" by us, our designees or any service firm paid for in whole or in part under this Cyber Coverage:

a. The effectiveness of such services depends on the cooperation and assistance of you, "affected individuals".

b. All services are available to all individuals but, depending on their circumstances, not all individuals will be able to benefit from them in the same way. For example, "affected individuals" who are minors or foreign nationals may not have credit records that can be provided or monitored. Service in Canada will be different from service in the United States and Puerto Rico in accordance with local conditions.

c. We do not warrant or guarantee that the services will end or eliminate all problems associated with the covered events.

d. You will have a direct relationship with the professional service firms paid for in whole or in part under this Cyber Coverage. Those firms work for you.

F. DEFINITIONS

1. "Affected Individual" means any person whose "personally identifying information" or "personally sensitive information" is lost, stolen, accidentally released or accidentally published by a "personal data compromise" covered under this Cyber Coverage. This definition is subject to the following provisions:

a. "Affected individual" does not include any business or organization. Only an individual person may be an "affected individual".

b. An "affected individual" may reside anywhere in the world.

2. "Authorized Third Party User" means a party who is not an employee or a director of you who is authorized by contract or other agreement to access the "computer system" for the receipt or delivery of services.

3. "Bodily Injury" means bodily injury, mental anguish, sickness or disease sustained by a person, including death resulting from any of these at any time.

4. "Business Income and Extra Expense Loss" means loss of Business Income and Extra Expense.

a. As used in this definition, Business Income means the sum of:

(1) Net income (net profit or loss before income taxes) that would have been earned or incurred; and

(2) Continuing normal and necessary operating expenses incurred, including employee and director payroll.

b. As used in this definition, Extra Expense means the additional cost you incur to operate your business over and above the cost that you normally would have incurred to operate your

business during the same period had no "computer attack" occurred.

5. "Claim"

a. "Claim" means:

(1) A written demand for monetary damages or non-monetary relief, including injunctive relief;

(2) A civil proceeding commenced by the filing of a complaint;

(3) An arbitration proceeding in which such damages are claimed and to which you must submit or do submit with our consent;

(4) Any other alternative dispute resolution proceeding in which such damages are claimed and to which you must submit or to which we agree you should submit to;

arising from a "wrongful act" or a series of interrelated "wrongful acts" including any resulting appeal.

b. "Claim" does not mean or include:

(1) Any demand or action brought by or on behalf of someone who is:

(a) Your director;

(b) Your owner or part-owner; or

(c) A holder of your securities;

in their capacity as such, whether directly, derivatively, or by class action. "Claim" will include proceedings brought by such individuals in their capacity as "affected individuals", but only to the extent that the damages claimed are the same as would apply to any other "affected individual"; or

(2) A "regulatory proceeding".

c. Includes a demand or proceeding arising from a "wrongful act" that is a "personal data compromise" only when the "affected individuals" were notified in compliance with applicable laws and regulations. A "personal data compromise" can qualify for coverage even if the "personal data compromise" is first discovered by you at the time that you receive notice of a "claim" or "regulatory proceeding". However, if the discovery of the "personal data compromise" first occurred following receipt of a "claim" or notice of suit, then notification to the "affected individuals" in compliance with applicable laws and regulations is not required as a prerequisite to coverage **4. Data Compromise Liability**.

6. "Computer Attack"

a. "Computer attack" means one of the following involving the "computer system":

(1) An "unauthorized access incident";

(2) A "malware attack"; or

(3) A "denial of service attack" against a "computer system".

b. A "computer attack" ends at the earlier of:

(1) The time that the active attacking behavior ceases, the time that you have regained control over the "computer system" or the time that all unauthorized creation, destruction or movement of data associated with the "computer attack" has ceased, whichever happens latest; or

(2) 30 days after your discovery of the "computer attack".

7. "Computer System" means a computer or other electronic hardware that:

a. Is owned or leased by you and operated under your control; or

b. Is operated by a third party service provider used for the purpose of providing hosted computer application services to you or for processing, maintaining, hosting or storing your electronic data, pursuant to a written contract with you for such services. However, such

computer or other electronic hardware operated by such third party shall only be considered to be a "computer system" with respect to the specific services provided by such third party to you under such contract.

8. **"Coverage Term"** means the increment of time:
   a. Commencing on the earlier of the first inception date of this Cyber Coverage or the first inception date of any coverage substantially similar to that described in this Cyber Coverage and held immediately prior to this Cyber coverage; and
   b. Ending upon the "termination of coverage".
9. **"Coverage Territory"** means:
   a. With respect to Data Compromise Response Expenses, Computer Attack and Cyber Extortion "coverage territory" means anywhere in the world.
   b. With respect to Data Compromise Liability, "coverage territory" means anywhere in the world, however "claims" must be brought within the United States (including its territories and possessions) or Puerto Rico.
10. **"Cyber Extortion Expenses"** means:
   a. The cost of a negotiator or investigator retained by you in connection with a "cyber extortion threat"; and
   b. Any amount paid by you in response to a "cyber extortion threat" to the party that made the "cyber extortion threat" for the purposes of eliminating the "cyber extortion threat" when such expenses are necessary and reasonable and arise directly from a "cyber extortion threat". The payment of "cyber extortion expenses" must be approved in advance by us. However, we will pay for "cyber extortion expenses" that have not been approved in advance by us if we determine that (1) it was not practical for you to obtain our prior approval, and (2) if consulted at the time, we would have approved the payment. We will not unreasonably withhold our approval.
11. **"Cyber Extortion Threat"** means:
   a. "Cyber extortion threat" means a demand for money from you based on a credible threat, or series of related credible threats, to:
      (1) Launch a "denial of service attack" against the "computer system" for the purpose of denying "authorized third party users" access to your services provided through the "computer system" via the Internet;
      (2) Gain access to a "computer system" and use that access to steal, release or publish "personally identifying information", "personally sensitive information" or "third party corporate data";
      (3) Alter, damage or destroy electronic data or software while such electronic data or software is stored within a "computer system";
      (4) Launch a "computer attack" against a "computer system" in order to alter, damage or destroy electronic data or software while such electronic data or software is stored within a "computer system"; or
      (5) Transfer, pay or deliver any funds or property using a "computer system" without your authorization.
   b. "Cyber extortion threat" does not mean or include any threat made in connection with a legitimate commercial dispute.
12. **"Data Re-creation Costs"**
   a. "Data re-creation costs" means the costs of an outside professional firm hired by you to research, re- create and replace data that has been lost or corrupted and for which there is no electronic source available or where the electronic source does not have the same or similar functionality to the data that has been lost or corrupted.
   b. "Data re-creation costs" does not mean or include costs to research, re-create or replace:

(1) Software programs or operating systems that are not commercially available; or

(2) Data that is obsolete, unnecessary or useless to you.

13. "Data Restoration Costs"

a. "Data restoration costs" means the costs of an outside professional firm hired by you to replace electronic data that has been lost or corrupted. In order to be considered "data restoration costs", such replacement must be from one or more electronic sources with the same or similar functionality to the data that has been lost or corrupted.

b. "Data restoration costs" does not mean or include costs to research, re-create or replace:

(1) Software programs or operating systems that are not commercially available; or

(2) Data that is obsolete, unnecessary or useless to you.

14. "Defense Costs"

a. "Defense costs" means reasonable and necessary expenses consented to by us resulting solely from the investigation, defense and appeal of any "claim" or "regulatory proceeding" against you. Such expenses may be incurred by us or paid by us on your behalf. Such expenses may include premiums for any appeal bond, attachment bond or similar bond. However, we have no obligation to apply for or furnish such bond.

b. "Defense costs" does not mean or include the salaries or wages of your employees or directors, or your loss of earnings.

15. "Denial of Service Attack" means an intentional attack against a target computer or network of computers designed to overwhelm the capacity of the target computer or network in order to deny or impede authorized users from gaining access to the target computer or network through the Internet.

16. "Identity Theft"

a. "Identity theft" means the fraudulent use of "personally identifying information". This includes fraudulently using such information to establish credit accounts, secure loans, enter into contracts or commit crimes.

b. "Identity theft" does not mean or include the fraudulent use of a business name, d/b/a or any other method of identifying a business activity.

17. "Loss"

a. With respect to Data Compromise Response Expenses, "loss" means those expenses enumerated in Data Compromise Response Expenses, paragraph **b**.

b. With respect to Computer Attack, "loss" means those expenses enumerated in Computer Attack, paragraph **b**.

c. With respect to Cyber Extortion, "loss" means "cyber extortion expenses".

d. With respect to Data Compromise Liability, "loss" means "defense costs" and "settlement costs".

18. "Malware Attack"

a. "Malware attack" means an attack that damages a "computer system" or data contained therein arising from malicious code, including viruses, worms, Trojans, spyware and key loggers.

b. "Malware attack" does not mean or include damage from shortcomings or mistakes in legitimate electronic code or damage from code installed on your "computer system" during the manufacturing process or normal maintenance.

19. "Period of Restoration" means the period of time that begins 8 hours after the time that a "computer attack" is discovered by you and continues until the earliest of:

a. The date that all data restoration, data re-creation and system restoration directly related to the "computer attack" has been completed;

b. The date on which such data restoration, data re-creation and system restoration could have been completed with the exercise of due diligence and dispatch; or

c. If no data restoration, data re-creation or system restoration is required, the end of the "computer attack".

20. "Personal Data Compromise" means the loss, theft, accidental release or accidental publication of "personally identifying information" or "personally sensitive information" as respects one or more "affected individuals". If the loss, theft, accidental release or accidental publication involves "personally identifying information", such loss, theft, accidental release or accidental publication must result in or have the reasonable possibility of resulting in the fraudulent use of such information. This definition is subject to the following provisions:

a. At the time of the loss, theft, accidental release or accidental publication, the "personally identifying information" or "personally sensitive information" need not be at the insured premises but must be in the direct care, custody or control of:

(1) You; or

(2) A professional entity with which you have a direct relationship and to which you (or an "affected individual" at your direction) have turned over (directly or via a professional transmission or transportation provider) such information for storage, processing, transmission or transportation of such information.

b. "Personal data compromise" includes disposal or abandonment of "personally identifying information" or "personally sensitive information" without appropriate safeguards such as shredding or destruction, provided that the failure to use appropriate safeguards was accidental and not reckless or deliberate.

c. "Personal data compromise" includes situations where there is a reasonable cause to suspect that such "personally identifying information" or "personally sensitive information" has been lost, stolen, accidentally released or accidentally published, even if there is no firm proof.

d. All incidents of "personal data compromise" that are discovered at the same time or arise from the same cause will be considered one "personal data compromise".

21. "Personally Identifying Information"

a. "Personally identifying information" means information, including health information, that could be used to commit fraud or other illegal activity involving the credit, access to health care or identity of an "affected individual". This includes, but is not limited to, Social Security numbers or account numbers.

b. "Personally identifying information" does not mean or include information that is otherwise available to the public, such as names and addresses.

22. "Personally Sensitive Information"

a. "Personally sensitive information" means private information specific to an individual the release of which requires notification of "affected individuals" under any applicable law.

b. "Personally sensitive information" does not mean or include "personally identifying information".

23. "Policy Period" means the period commencing on the effective date shown in the Cyber Suite Supplemental Declarations. The "policy period" ends on the expiration date or the cancellation date of this Cyber Coverage, whichever comes first. If there is a "termination of coverage" as described in paragraph **b.** of the definition of "termination of coverage", the policy period will be understood to end on the date of such change, but only with respect to such changed coverage.

24. "Property Damage" means

a. Physical injury to or destruction of tangible property including all resulting loss of use; or

b. Loss of use of tangible property that is not physically injured.

25. "Regulatory Proceeding" means an investigation, demand or proceeding alleging a violation of law or regulation arising from a "personal data compromise" brought by, or on behalf of, the Federal Trade Commission, Federal Communications Commission or other administrative or regulatory agency, or any federal, state, local or foreign governmental entity in such entity's regulatory or official capacity.

26. "Settlement Costs"

a. "Settlement costs" means the following, when they arise from a "claim":

(1) Damages, judgments or settlements; and

(2) Attorney's fees and other litigation costs added to that part of any judgment paid by us, when such fees and costs are awarded by law or court order; and

(3) Pre-judgment interest on that part of any judgment paid by us.

b. "Settlement costs" does not mean or include:

(1) Civil or criminal fines or penalties imposed by law;

(2) Punitive and exemplary damages;

(3) The multiple portion of any multiplied damages;

(4) Taxes; or

(5) Matters which may be deemed uninsurable under the applicable law.

27. "System Restoration Costs"

a. "System restoration costs" means the costs of an outside professional firm hired by you to do any of the following in order to restore your "computer system" to its pre-"computer attack" level of functionality:

(1) Replace or reinstall computer software programs;

(2) Remove any malicious code; and

(3) Configure or correct the configuration of your "computer system".

b. "System restoration costs" does not mean or include:

(1) Costs to increase the speed, capacity or utility of a "computer system" beyond what existed immediately prior to the "computer attack";

(2) Labor costs of your employees or directors;

(3) Any costs in excess of the actual cash value of your "computer system"; or

(4) Costs to repair or replace hardware.

28. "Termination of Coverage", as respects Third Party Coverages only, means, whether made by the insurer or the insured at any time:

a. Cancellation or nonrenewal of a policy; or

b. Decrease in limits, reduction of coverage, increased deductible or self-insured retention, new exclusion, or any other change in coverage less favorable to the insured.

29. "Third Party Corporate Data"

a. "Third party corporate data" means any trade secret, data, design, interpretation, forecast, formula, method, practice, credit or debit card magnetic strip information, process, record, report or other item of information of a third party not an insured under this Cyber Coverage which is not available to the general public and is provided to you subject to a mutually executed written confidentiality agreement or which you are legally required to maintain in confidence.

b. "Third party corporate data" does not mean or include "personally identifying information" or "personally sensitive information".

30. "Unauthorized Access Incident" means the gaining of access to a "computer system" by:

a. An unauthorized person or persons; or

b. An authorized person or persons for unauthorized purposes.

31. "Wrongful Act" means, with respect to Data Compromise Liability, a "personal data compromise".

All other terms and conditions remain unchanged.