Insured Copy
Erie Insurance Company
NAIC Code 26263

Erie Insurance®

Coverage provided by
Erie Insurance Company
100 Erie Insurance Place Erie, PA 16530
erieinsurance.com

ErieSecure Business™ Policy Declarations

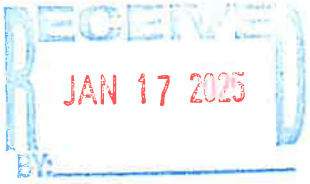
Amended Declarations
See * Notice of Amendment**
Effective 01/06/2025 Attach This To Your Policy

Mailing name and address for Insured
MCCORD POINTE HOMEOWNERS ASSOCIATION INC
11711 N COLLEGE AVE STE 100
CARMEL IN 46032-5601

Other Interest
As listed under Schedule of Other Interests

Named Insured's full name
McCord Pointe Homeowners Association Inc.

112846457
FF1054



Legal entity
Association

Agent		Policy period	Policy number
FF2563	STEFFEY INSURANCE AGENCY	10/14/2024 to 10/14/2025	Q61 0465515

Agent address and phone

STEFFEY INSURANCE AGENCY
3091 E 98TH ST STE 125
INDIANAPOLIS, IN 46280-2910
(800) 881-9731

Policy period begins at 12:01 A.M. standard time on the effective date and ends at 12:01 A.M. standard time on the expiration date. Standard time is determined at the stated address of the Named Insured.

Agency email address

mail@steffeyins.com

Agency website

http://www.steffeyins.com

Policy Change - ***Notice of Amendment

Change effective date: 01/06/2025

Customer information
Changed
Preferred contact information
From Teanna Adcock 3179143275 kstallworth@cas-indiana.com
To Kelly Stallworth 3179143275 kstallworth@cas-indiana.com
Phone from 3172531401 to 3179143275
Email from tadcock@ardsleymgmt.com to kstallworth@cas-indiana.com
Address Line 1 from 3002 E 56TH ST to 11711 N COLLEGE AVE STE 100
City name from INDIANAPOLIS to CARMEL
Postal code from 46220-2946 to 46032-5601

Policy information
Changed
Address from 3002 E 56TH ST, INDIANAPOLIS, IN 46220-2946 to 11711 N COLLEGE AVE STE 100, CARMEL, IN 46032-5601
Phone from 3172531401 to 3179143275
Email from tadcock@ardsleymgmt.com to kstallworth@cas-indiana.com
Billing information
Renewal billing address from 3002 E 56TH ST, INDIANAPOLIS, IN 46220-2946 to 11711 N COLLEGE AVE STE

10337

Policy Change - ***Notice of Amendment

100, CARMEL, IN 46032-5601
Billing address from 3002 E 56TH ST, INDIANAPOLIS, IN 46220-2946 to 11711 N COLLEGE AVE STE 100, CARMEL, IN 46032-5601
Other interests
Community Association Service of Indiana
Added
Mailing name 2: of Indiana
Changed
Address from 3002 E 56TH ST, INDIANAPOLIS, IN 46220-2946 to 11711 N COLLEGE AVE STE 100, CARMEL, IN 46032-5601
Mailing name 1 from Ardsley Management to Community Association Service

Premium Summary

No difference in premium due to this change
Total annual policy premium $7,062.00

Schedule of Forms

Form number	Edition date	Description
CG0001	04/13	Commercial General Liability Coverage Form
CG0123	03/97	Indiana Changes - Pollution Exclusion
CG2011	04/13	Additional Insured - Managers or Lessors of Premises
CG2106	05/14	Exclusion - Access or Disclosure of Confidential or Personal Information and Data-Related Liability - With Limited Bodily Injury Exception
CG2109	06/15	Exclusion - Unmanned Aircraft
CG2146	07/98	Abuse or Molestation Exclusion
CG2170	01/15	Cap on Losses from Certified Acts of Terrorism
CG4032	05/23	Exclusion - Perfluoroalkyl and Polyfluoroalkyl Substances (PFAS)
EPP0001	10/22	ErieSecure Business Property Coverage Part
EPP0006	10/19	ErieSecure Business Extra Liability Coverages
EPP0008	09/23	Policy Change Endorsement - Exclusions
EPP0009	10/19	Exclusion - Professional Liability
EPP0011IN	10/19	Indiana Liability Change Endorsement
EPP0027	10/19	Important Notice to Indiana Policyholders - ErieSecure Business
EPP0094	10/24	Premium Audit - Noncompliance Charge
EPP0218	10/19	Sewer and Drain Back-Up
EPP0236	10/22	Agreed Amount Clause
EPP1804	10/19	Additional Insured - Homeowners, Townhouse, or Similar Association
EPP2903	10/19	Identity Recovery - Owners and Employees
EPP2905	10/19	Employee Dishonesty - Increased Coverage
EPP3208	10/19	Exclusion - Lead Liability
EPP3218	10/19	Exclusion - Data Breach Response Expenses
EPP4000IN	11/21	ErieSecure Business Policy - Indiana
EPP4001	10/19	Amendment of Mobile Equipment Definition
EPP4002	10/22	Pollutants Redefined
EPP4007	10/19	Coverage for Punitive Damages
EPP4500	12/21 *	Cyber Suite Coverage
EPP4502IN	12/21	Cyber Suite - Indiana Changes Amendatory Endorsement
EPP4503	12/21 *	Important Notice - Cyber Coverage Resources Available

CONTINUED ON NEXT PAGE

Schedule of Forms - *(continued)*

Form number	Edition date	Description
IL952A	03/21	Cap on Losses from Certified Acts of Terrorism
IL985H	03/21	Disclosure Pursuant to Terrorism Risk Insurance Act

CYBER SUITE COVERAGE

Various provisions in this Coverage Form restrict coverage. Read the entire Coverage Form carefully to determine rights, duties, and what is and is not covered.

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

The word "insured" means any person or organization qualifying as such under **Section III – WHO IS AN INSURED**.

Other words and phrases that appear in quotations have special meaning. Refer to **Section VII – CYBER SUITE COVERAGE DEFINITIONS**.

The terms and conditions of the Cancellation Clause of the ErieSecure Business General Policy Conditions 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.

SECTION I – COVERAGES

1. **Data Breach Response Expenses**

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

      1) There has been a "personal data breach";

      2) Such "personal data breach" took place in the "coverage territory";

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

      4) Such "personal data breach" is reported to us as soon as practicable, but in no event more than sixty (60) days 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 breach" and are necessary and reasonable. Items **4)** and **5)** below apply only if there has been a notification of the "personal data breach" 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 breach" and the number and identities of the "affected individuals". This includes, when necessary, the cost of a qualified Payment Card Forensic Investigator.

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

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

         b) 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 breach" 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 breach". However, once it is determined that there was no covered "personal data breach", we will not pay for any further costs.

      2) **Legal Review**

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

         If there is reasonable cause to suspect that a covered "personal data breach" 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 breach". However, once it is determined that there was no covered "personal data breach", 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 breach" 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 breach" 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 breach". 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 breach", 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.

5) **Public Relations**

We will pay for a professional public relations firm review of, and response to, the potential impact of the "personal data breach" 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".

6) **Regulatory Fines and Penalties**

We will pay for any fine or penalty imposed by law, to the extent such fine or penalty is legally insurable under the law of the applicable jurisdiction. This includes, but is not limited to, fines and penalties imposed for the violation of the European Union General Data Protection Regulation, the California Consumer Privacy Act, and similar laws.

7) **PCI Assessments, Fines and Penalties**

We will pay for any Payment Card Industry assessments, fines, and penalties imposed on you under a contract to which you are a party.

This does not include any:

a) Increased transaction costs;

b) Any assessments, fines, and penalties not arising from a covered "personal data breach";

c) Interchange fees;

d) Chargebacks;

e) Subsequent assessments, fines, and penalties imposed due to continued PCI non-compliance; or

f) Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.

8) **Reputational Harm**

This Reputational Harm coverage applies only if there has been a "personal data breach" for which you provided notifications and services to "affected individuals" in consultation with us pursuant to **b.3)** and **b.4)** above.

If the conditions listed in **a)** above have been met, then we will pay your necessary and reasonable "reputational harm costs" incurred during the "period of indemnification" and arising directly from the "personal data breach".

9) **Reward Payments**

We will pay for any necessary and reasonable "reward payments" offered and made by you in response to a "personal data breach".

2. **Computer Attack**

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

1) There has been a "computer attack";

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

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

4) Such "computer attack" is reported to us as soon as practicable, but in no event more than sixty (60) days 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 cost".

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". This includes your actual "business income and extra expense loss" caused by a voluntary shutdown of your "computer system" in connection with your reasonable efforts to stop, mitigate the effects of, or recover from, such a "computer attack".

5) **Extended Income Recovery**

If you suffer a covered "business income and extra expense loss" resulting from a "computer attack" on a "computer system" owned or leased by you and operated under your control, we will pay your actual "extended income loss".

6) **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.

7) **Future Loss Avoidance**

If you received a loss payment from us under Coverage **2. Computer Attack**, we will pay your necessary and reasonable "future loss avoidance costs".

8) **Reward Payments**

We will pay for any necessary and reasonable "reward payments" offered and made by you in response to a "computer attack".

3. **Cyber Extortion**

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

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

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, but in no event more than sixty (60) days 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" and any necessary and reasonable "reward payments" offered and made by you in response to a "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 our approval.

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

4. **Misdirected Payment Fraud**

a. Misdirected Payment Fraud applies only if all of the following conditions are met:

1) There has been a "wrongful transfer event" against you;

2) Such "wrongful transfer event" took place in the "coverage territory";

3) Such "wrongful transfer event" is first discovered by you during the "policy period";

4) Such "wrongful transfer event" is reported to us as soon as practicable, but in no event more than sixty (60) days after the date it is first discovered by you; and

5) Such "wrongful transfer event" is reported in writing by you to the police.

b. If the conditions listed above in **a.** above have been met, then we will pay your necessary and reasonable "wrongful transfer costs" arising directly from the "wrongful transfer event" and any necessary and reasonable "reward payments" offered and made by you in response to a "wrongful transfer event".

5. **Computer Fraud**

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

1) There has been a "computer fraud event" against you;

2) Such "computer fraud event" took place in the "coverage territory";

3) Such "computer fraud event" is first discovered by you during the "policy period";

4) Such "computer fraud event" is reported to us within sixty (60) days after the date it is first discovered by you; and

5) Such "computer fraud event" is reported in writing by you to the police.

b. If the conditions listed in **a.** above have been met, then we will pay your necessary and reasonable "computer fraud costs" arising directly from the "computer fraud event" and any necessary and reasonable "reward payments" offered and made by you in response to a "computer fraud event".

6. **Telecommunications Fraud**

   a. Telecommunications Fraud applies only if all of the following conditions are met:

      1) There has been a "computer attack" on a "telecommunications system" that is owned or leased by you and operated under your control;

      2) Such "computer attack" took place in the "coverage territory";

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

      4) Such "computer attack" is reported to us within sixty (60) days after the date it is first discovered by you;

      5) Such "computer attack" is reported in writing by you to the police; and

      6) As a result of such "computer attack", there have been "telecommunications fraud costs".

   b. If the conditions listed in **a.** above have been met, then we will pay your necessary and reasonable "telecommunications fraud costs" arising directly from the "computer attack".

7. **Privacy Incident Liability**

   a. Privacy Incident 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"; or

         b) A "regulatory proceeding".

      2) Such "claim" or "regulatory proceeding" must arise from a "privacy incident" that:

         a) Took place during the "coverage term";

         b) Took place in the "coverage territory"; and

         c) Was submitted to us and insured under Data Breach Response Expenses.

      3) Such "claim" or "regulatory proceeding" is reported to us as soon as practicable, but in no event more than sixty (60) days 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 "privacy incident" or interrelated "privacy incidents" 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.

8. **Network Security Liability**

   a. Network Security 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 a "claim" which arises from a "network security incident" that:

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

         b) Took place in the "coverage territory"; and

      2) Such "claim" is reported to us as soon as practicable, but in no event more than sixty (60) days 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 "loss" directly arising from the "claim".

   c. All "claims" arising from a single "network security incident" or interrelated "network security incidents" will be deemed to have been made at the time that notice of the first of those "claims" is received by you.

9. **Electronic Media Liability**

   a. Electronic Media 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 a "claim" which arises from an "electronic media incident" that:

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

         b) Took place in the "coverage territory"; and

      2) Such "claim" is reported to us as soon as practicable, but in no event more than sixty (60) days 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 "loss" directly arising from the "claim".

   c. All "claims" arising from a single "electronic media incident" or interrelated "electronic media incidents" will be deemed to have been made at the time that notice of the first of those "claims" is received by you.

SECTION II – EXCLUSIONS

This Insurance does not apply to:

1. Nuclear reaction or radiation or radioactive contamination, however caused.
2. 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.
3. 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.
4. Any attack on, incident involving, or loss to any computer or system of computers that is not a "computer system".
5. Costs to research or correct any deficiency.
6. Any fines or penalties other than those explicitly covered under Data Breach Response Expenses.
7. Any criminal investigations or proceedings.
8. Your intentional or willful complicity in a covered "loss" event.
9. 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.
10. Any liability arising out of any dishonest, fraudulent, criminal, or malicious act by or at the direction of any insured. However, to the extent that a "claim" or "suit" is otherwise covered under this Coverage Form, we will defend a "claim" or "suit" asserting a dishonest, fraudulent, or malicious act until such time as the insured is determined to have committed such dishonest, fraudulent, or malicious act.

    The "wrongful act(s)" of an insured shall not be imputed to any other insured for the purpose of determining the applicability of this exclusion.
11. Any liability arising out any "personal data breach", "computer attack", cyber extortion threat", "wrongful transfer event", "computer fraud event", or "wrongful act" which an insured:
    a. Had knowledge of; or
    b. Could have reasonably foreseen might result in a "claim" or "suit"

    and which were known to the insured prior to the effective date of this Cyber Coverage or the first Cyber Coverage issued by us for which this Cyber Coverage is an uninterrupted renewal.
12. Any liability of others assumed by the insured under any contract or agreement, whether oral or in writing.

    This exclusion, however, shall not apply to any liability for damages that the insured would have in the absence of such contract or agreement
13. Any liability arising out of the facts alleged, or to the same "wrongful employment acts" alleged or contained in any "claim" or "suit" which has been reported, or in any circumstances for which notice has been given, under any policy for which this Cyber Coverage is a renewal or replacement.
14. Any liability arising out of any prior:
    a. Litigation; or
    b. Administrative or regulatory proceeding or investigation

    for which an insured had notice, or alleging the same "wrongful acts" alleged or contained in such pending or prior litigation or administrative or "regulatory proceeding" or investigation which the insured had knowledge of prior to the effective date of this Cyber Coverage or the first Cyber Coverage issued by us for which this Cyber Coverage is an uninterrupted renewal.
15. 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".
16. The propagation or forwarding of malware, including viruses, worms, Trojans, spyware, and keyloggers in connection with hardware or software created, produced, or modified by you for sale, lease, or license to third parties.
17. Any "claim" or "loss" alleging, arising out of, based upon or attributable to, or brought by or on behalf of any federal, state, or legal government agency or professional or trade licensing organizations or the enforcement of any governmental law, ordinance, regulation, or rule; however, this exclusion shall not apply to:
    a. Actions or proceedings brought by a governmental authority or regulatory agency acting solely in its capacity as your customer;
    b. "Regulatory proceedings" insured under Paragraph **7. Privacy Incident Liability** under **Section I – Coverages**; or

c. Any fine or penalty imposed by law which arises from a covered "personal data breach".

18. Any "loss" or liability arising out of "pollutants or contaminants" or the presence of or the actual, alleged, or threatened discharge, dispersal, release, or escape of "pollutants or contaminants", or any direction or request to test for, monitor, clean up, remove, contain, treat, detoxify, or neutralize "pollutants or contaminants", or in any way respond to or assess the effects of "pollutants or contaminants".

19. Any oral or written publication of material, if done by you or at your direction with knowledge of its falsity.

20. "Property damage" or "bodily injury" other than mental anguish or mental injury alleged in a "claim" covered under Privacy Incident Liability, Network Security Liability, or Electronic Media Liability.

21. This insurance does not apply to:

    a. Any "future loss avoidance costs" incurred after this policy has been cancelled or non-renewed by either you or us.

    b. The salaries or wages of your "employees" or "executives", or your loss of earnings.

22. Any amount not insurable under applicable law.

23. Any violation of U.S. economic or trade sanctions.

SECTION III – WHO IS AN INSURED

1. For purposes of this insurance, if you are designated in the Declarations as:

    a. An individual, you and your spouse or "domestic partner are insureds, but only with respect to the conduct of a business of which you are the sole owner.

    b. A partnership or joint venture, you are an insured. Your current or former members, your partners, and their spouses or "domestic partners" are also insureds, but only with respect to the conduct of your business.

    c. A limited liability company, you are an insured. Your current or former members are also insureds, but only with respect to the conduct of your business. Your current or former managers are insureds, but only with respect to their duties as your managers.

    d. A corporation or organization other than a partnership, joint venture, or limited liability company, you are an insured. Your current or former directors are insureds, but only with respect to their duties as your directors.

    e. A trust, you are an insured. Your current or former trustees are also insureds, but only with respect to their duties as trustees.

2. Each of the following is also an insured:

    a. Your current or former "employees", executive officers, and directors are insureds, but only for acts within the scope of their employment by you or while performing duties with respect to the conduct of your business or with respect to their duties as executive officers or directors.

    b. Estates, heirs, or legal representative of deceased individual insureds, and the legal representatives of individual insureds, in the event of incompetency, who were individual insureds at the time the "wrongful employment acts", upon which such "claims" or "suits" are based, were committed.

3. Any organization you newly acquire or form, other than a partnership, joint venture, or limited liability company, and over which you maintain ownership or majority interest, will qualify as a Named Insured if there is no other similar insurance available to that organization. However:

    a. Coverage under this provision is afforded only until the 90th day after you acquire or form the organization or the end of the "policy period", whichever is earlier;

    b. Coverage does not apply to "wrongful employment acts" that were committed or existed before you acquired or formed the organization; and

    c. The organization must be engaged in the business capacity described in the Declarations.

    No person or organization is an insured with respect to the conduct of any current or past partnership, joint venture, or limited liability company that is not shown as a Named Insured in the Declarations.

SECTION IV – LIMITS OF INSURANCE

1. **Aggregate Limits.**

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

2. **Coverage Sublimits**

    a. **Data Breach Sublimits**

    The most we will pay under Data Breach Response Expenses for Public Relations and Reputational Harm coverages for "loss" arising from any one "personal data breach" is the applicable sublimit for each of those coverages shown in the Declarations.

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

b. **Computer Attack Sublimit**

The most we will pay under Computer Attack for Public Relations coverage for "loss" arising from any one "computer attack" is the applicable Public Relations sublimit shown in the Declarations. This sublimit is part of, and not in addition to, the Cyber Suite Annual Aggregate Limit shown in the 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 Declarations. This sublimit is part of, and not in addition to, the Cyber Suite Annual Aggregate Limit shown in the Declarations.

d. **Misdirected Payment Fraud Sublimit**

The most we will pay under Misdirected Payment Fraud coverage for "loss" arising from one "wrongful transfer event" is the applicable sublimit shown in the Declarations. This sublimit is part of, and not in addition to, the Cyber Suite Annual Aggregate Limit shown in the Declarations.

e. **Computer Fraud Sublimit**

The most we will pay under Computer Fraud coverage for "loss" arising from one "computer fraud event" is the applicable sublimit shown in the Declarations. This sublimit is part of, and not in addition to, the Cyber Suite Annual Aggregate Limit shown in the Declarations.

f. **Telecommunications Fraud Sublimit**

The most we will pay under Telecommunications Fraud coverage for "loss" arising from one "computer attack" on a "telecommunications system" is the applicable limit shown in the Declarations. This sublimit is part of, and not in addition to, the Cyber Suite Annual Aggregate Limit shown in the Declarations.

g. **Reward Payments Sublimit**

The Reward Payment sublimit shown in the Declarations is the most we will pay for all "reward payments" resulting from a "personal data breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event" in any one "policy period".

This sublimit is a part of, and not in addition to, the Cyber Suite Annual Aggregate Limit shown in the Declarations.

3. **Application of Limits**

a. A "computer attack", "cyber extortion threat", "personal data breach", "wrongful transfer event", or "computer fraud event" 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", "personal data breach", "wrongful transfer event", or "computer fraud event" will be subject to the limit of insurance applicable to the "policy period" when the "computer attack", "cyber extortion threat", "personal data breach", "wrongful transfer event", or "computer fraud event" 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.

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 Breach 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.

SECTION V – DEDUCTIBLES

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

2. The deductible will apply to all:

   a. "Loss" arising from the same insured event or interrelated insured events under Data Breach Response Expenses, Computer Attack, Cyber Extortion, Misdirected Payment Fraud, Computer Fraud, or Telecommunications Fraud coverage.

   b. "Loss" resulting from the same "wrongful act" or interrelated "wrongful acts" insured under Privacy Incident Liability, Network Security Liability, or Electronic Media Liability.

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

SECTION VI – CYBER SUITE COVERAGE CONDITIONS

1. **Additional Policy Protection**

   We may, from time to time, offer or arrange to provide benefits specific to one of our risk management benefits which include but are not limited to devices, equipment, services, or benefits provided by either us or a third party vendor selected by us. These services or products are designed to mitigate loss, provide loss control, assess risk, identify sources of risk, or develop strategies for eliminating or reducing risk. The benefits are intended to enhance the safety, value, usability, life, or protection of you or your insurable assets. Such products or services must be provided by us or by a third party vendor that has an agreement or contract with us. We do not warrant the merchantability, fitness, or quality of any product or service offered or provided by that organization.

2. **Bankruptcy**

   The bankruptcy or insolvency of you or your estate, will not relieve you or us of any obligation under this Cyber Coverage.

3. **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. 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. At the time a "claim" or "regulatory proceeding" is first reported to us, you may request that we appoint a defense attorney of your choice. We will give full consideration to any such request.

   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. We may, with your written consent, make any settlement of a "claim" or "regulatory proceeding" which we deem reasonable. If you refuse to consent to any settlement recommended by us and acceptable to the claimant or plaintiff, our liability for all "settlement costs" and "defense costs" resulting from such "claim" or "regulatory proceeding" will not exceed the following:

      1) The amount for which we could have settled such "claim" or "regulatory proceeding" plus "defense costs" incurred as of the date we proposed such settlement in writing to you; plus

      2) 80% of any "settlement costs" and "defense costs" incurred after the date of such proposed settlement;

      subject to the applicable limits.

4. **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.

5. **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 and either:

      1) Anytime during the "policy period"; or

      2) Anytime during the extended reporting periods (if applicable).

IMPORTANT NOTICE – CYBER RESOURCES AVAILABLE

Thank you for purchasing Cyber Suite coverage from ERIE. We appreciate the trust you have placed in us.

As an ERIE Cyber Suite customer, we're happy to offer you access to the following resources:

eRiskHub® Website

This website provides resources to help you identify and protect your team from cyber risks, such as an incident response roadmap, an eRisk resources directory, an online, ready-to-use training module, a learning center, risk management tools, and a news center.

The general information and materials provided on the website do not represent legal advice and are not meant to be a substitute for seeking competent legal and/or professional cyber security advice.

To gain access to the website, visit: **https://eriskhub.com/erieinsurance**

- For Access Code, enter: **12116-196**
- Complete the entire registration form by creating a username and password.
- Log In: After registering, log in with your username and password.
- Navigate: Use your access to explore all that the eRiskHub® has to offer including cyber news and helpful guides on breaches, technical support, reporting a loss and more!

Cyber Safety Website

This website provides resources such as Cybersecurity training to help you protect your team from cyber risks, security policy templates to help you identify and document compliance with multiple regulations, and web app security scans to help you identify potential security weaknesses in your business.

The general information and materials provided on the website do not represent legal advice and are not meant to be a substitute for seeking competent legal and/or professional cyber security advice.

To gain access to the website, visit: **https://zeguro.com/erieinsurance**

- Complete the registration by using your email address and creating a password to sign up.
- Verify your email address.
- Answer a short survey regarding your company to complete the registration.

Thank you again for being an ERIE customer. We hope you find our services valuable in helping to protect your and your business.

51. **"Wrongful Act"**

    a. With respect to Privacy Incident Liability, "wrongful act" means a "privacy incident";

    b. With respect to Network Security Liability, "wrongful act" means a "network security incident"; and

    c. With respect to Electronic Media Liability, "wrongful act" means an "electronic media incident".

52. **"Wrongful Transfer Costs"** means the amount of "money" fraudulently obtained from you. "Wrongful transfer costs" include the direct financial loss only. "Wrongful transfer costs" do not include any of the following:

    a. Other expenses that arise from the "wrongful transfer event";

    b. Indirect loss, such as "bodily injury", lost time, lost wages, identity recovery expenses, or damaged reputation;

    c. Any interest, time value, or potential investment gain on the amount of financial loss; or

    d. Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.

53. **"Wrongful Transfer Event"**

    a. "Wrongful transfer event" means an intentional and criminal deception of you or a financial institution with which you have an account. The deception must be perpetrated by a person who is not an "employee", "executive", or "independent contractor" using email, facsimile, or telephone communications to induce you or the financial institution to send or divert "money", "securities", or tangible property. The deception must result in direct financial loss to you.

    b. "Wrongful transfer event" does not mean or include any occurrence:

        1) In which you are threatened or coerced to send money or divert a payment; or

        2) Arising from a dispute or disagreement over the completeness, authenticity, or value of a product, a service, or a financial instrument.

b. "Securities" does not mean or include "money".

44. **"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-judgement 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, except for civil fines and penalties expressly covered under Data Breach Response Expenses;

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.

c. With respect to fines and penalties, the law of the jurisdiction most favorable to the insurability of those fines, or penalties will control for the purpose of resolving any dispute between us and you regarding whether the fines, or penalties specified in this definition above are insurable under this Cyber Coverage, provided that such jurisdiction:

1) Is where those fines, or penalties were awarded or imposed;

2) Is where any "wrongful act" took place for which such fines, or penalties were awarded or imposed;

3) Is where you are incorporated or you have your principal place of business; or

4) Is where we are incorporated or have our principal place of business.

45. **"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. However, at our sole discretion, we may choose to pay to repair or replace hardware if doing so reduces the amount of "loss" payable under this Cyber Coverage.

46. **"Telecommunications Fraud Costs"** means any payment that you are responsible for making to your Telephone Service Provider as a result of a "computer attack" on a "telecommunications system" that is owned or leased by you and operated under your control. As used in this definition, Telephone Service Provider means a business with which you have a written contract to provide you with telephone services.

47. **"Telecommunications System"** means any telephone or fax system including but not limited to, Voice over Internet Protocol (VoIP) or other internet-based telephone system is owned or leased by you and operated under your control.

48. **"Termination of Coverage"** means:

a. You or we cancel this coverage;

b. You or we refuse to renew this coverage; or

c. We renew this coverage on an other-than-claims-made basis or with a retroactive date later than the date of the first inception of this coverage or any coverage substantially similar to that described in this Cyber Coverage.

49. **"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".

50. **"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.

37. **"Pollutants or Contaminants"** include, but are not limited to, any solid, liquid, gaseous, biological, radiological, or thermal irritant or contaminant, including smoke, vapor, dust, fibers, mold, spores, fungi, bacterium, microorganism, virus, or other pathogen, diseases, germs, soot, fumes, asbestos, acids, alkalis, chemicals, and waste. Waste includes, but is not limited to, materials to be recycled, reconditioned, or reclaimed and nuclear materials.

38. **"Privacy Incident"** means:

    a. A "personal data breach";

    b. Your failure to comply with a Privacy Policy;

    c. Your unauthorized, unlawful (including, but not limited to, in violation of the European Union General Data Protection Regulation, the California Consumer Privacy Act, or similar laws), or wrongful collection of "personally identifying information"; or

    d. Your unlawful (including, but not limited to, in violation of the European Union General Data Protection Regulation, the California Consumer Privacy Act, or similar laws) or wrongful failure to amend, correct, or delete "personally identifying information".

    For the purpose of this definition, Privacy Policy means a publicly available written policy formally adopted by you which addresses the collection, handling, and management of "personally identifying information".

39. **"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.

40. **"Regulatory Proceeding"** means an investigation, demand, or proceeding alleging a violation of law or regulation arising from a "personal data breach" 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.

41. **"Reputational Harm Costs"**

    a. "Reputational harm costs" means the loss of Business Income during the "period of indemnification" arising directly from damage to your reputation caused by a "personal data breach".

        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 "executive" payroll.

    b. "Reputational harm costs" does not mean or include Business Income you lose due to:

        1) Unfavorable or deteriorated business conditions;

        2) Decreased market share;

        3) Any other consequential damages or losses;

        4) Legal costs or expenses;

        5) Investment income;

        6) Bank interest;

        7) Seasonal fluctuations; or

        8) Additional costs you incur to operate your business over and above the costs that you normally would have incurred to operate your business during the same period had no "personal data breach" occurred.

42. **"Reward Payments"** means:

    An amount of "money" paid by you to any individual(s) for information leading to the arrest and conviction of any perpetrator(s) of a "personal data breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event" that:

    a. We agree to in writing prior to the "reward payments" being offered or paid; and

    b. Are offered and paid prior to the earlier of:

        1) Six months after the "personal data breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event". or

        2) Expiration of the policy term.

        Such individual may not be:

        1) You;

        2) Your employee;

        3) Anyone hired by you to investigate a "personal data breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event". or

        4) A member of law enforcement.

43. **"Securities"**

    a. "Securities" means:

        1) Written negotiable and non-negotiable instruments or contracts representing "money" or tangible property; or

        2) Uncertified securities.

bullion, travelers' checks, registered checks, and money orders held for sale to the public.

b. "Money" does not mean or include any cryptocurrency, whether or not authorized or adopted by a domestic or foreign government. Cryptocurrency includes, but is not limited to, Bitcoin, Ethereum, and other forms of digital, virtual, or electronic currency.

30. **"Network Security Incident"** means a negligent security failure or weakness with respect to a "computer system" which allowed one or more of the following to happen:

    a. The unintended propagation or forwarding of malware, including viruses, worms, Trojans, spyware, and keyloggers. Malware does not include shortcomings or mistakes in legitimate electronic code;

    b. The unintended abetting of a "denial of service attack" against one or more other systems; or

    c. The unintended loss, release, or disclosure of "third party corporate data".

31. **"Period of Indemnification"** means the period of time that begins on the date you first provided notification to "affected individuals" pursuant to Paragraph **1. Data Response Expenses** under **Section I – Coverages** and ends after thirty (30) days.

32. **"Period of Restoration"** means the period of time that begins eight (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;

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

    d. 180 days after the "computer attack" is discovered by you.

33. **"Personal Data Breach"** 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 breach" 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 breach" 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 breach" that are discovered at the same time or arise from the same cause will be considered one "personal data breach".

34. **"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.

35. **"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".

36. **"Policy Period"** means the period commencing on the effective date shown in the Declarations. The "policy period" ends on the expiration date or the cancellation date of this Cyber Coverage, whichever comes first.

4) General Partner;

5) Member (if a limited liability company);

6) Manager (if a limited liability company); or

7) Trustee;

of your business.

22. **"Extended Income Loss"** means your actual "business income and extra expense loss" incurred during the "extended recovery period".

23. **"Extended Recovery Period"** means a fixed period of one hundred-eighty (180) days immediately following the end of the "period of restoration".

24. **"Future Loss Avoidance Costs"**

a. "Future loss avoidance costs" means the amount you spend to make improvements to a "computer system" owned or leased by you and operated under your control, provided:

1) Such "future loss avoidance costs" are incurred within thirty (30) days after your discovery of the "computer attack"; and

2) We agree in writing that improvements to which "future loss avoidance costs" relate would reasonably reduce the likelihood of a future "computer attack" similar to the one for which you have received payment under Paragraphs **2.b.1) through 2.b.4)** under **Section I – Coverages**. We will not unreasonably withhold such agreement; and

3) We receive your invoices for the "future loss avoidance costs" no later than sixty (60) days after the date you received the payment for the loss under Paragraphs **2.b.1) through 2.b.4)** under **Section I – Coverages**.

b. The most we will pay for all "future loss avoidance costs" with respect to any one "computer attack" is 10% of our Eligible Payment to you prior to any payment under this Future Loss Avoidance coverage. Any portion of the payment made for hardware replacement or hardware upgrades reduces the amount we will pay.

c. The improvements described in paragraph **a.2)** may include, but are not limited to, hardware and software upgrades. Improvements involving services subject to lease, license, or subscription may have costs that are ongoing. In such case, the most we will pay are costs associated with the first twelve (12) months of any such service, subject to the amount described in paragraph **b.** above.

d. As used in this coverage, Eligible Payment means our total payment to you under Paragraphs **2.b.1) through 2.b.4)** under **Section I – Coverages**, not including any deductible amount.

25. **"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.

26. **"Independent Contractor"** means a natural person that provides goods or services to you under terms specified in a written contract, but only while acting on behalf of, at the direction of, and under the supervision of you.

27. **"Loss"**

a. With respect to Data Breach Response Expenses, "loss" means those expenses enumerated Paragraph **1.b.** under **Section I – Coverages**.

b. With respect to Computer Attack, "loss" means those expenses enumerated in Paragraph **2.b.** under **Section I – Coverages**.

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

d. With respect to Misdirected Payment Fraud, "loss" means "wrongful transfer costs".

e. With respect to Computer Fraud, "loss" means "computer fraud costs".

f. With respect to Telecommunications Fraud, "loss" means "telecommunications fraud costs".

g. With respect to Privacy Incident Liability, Network Security Liability, and Electronic Media Liability, "loss" means "defense costs" and "settlement costs".

28. **"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 keyloggers.

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.

29. **"Money"** means:

a. "Money" means a medium of exchange in current use and authorized or adopted by a domestic or foreign government, including currency, coins, banknotes,

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.

14. **"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.

15. **"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.

16. **"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 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.

17. **"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.

18. **"Domestic Partner"** means any natural person legally recognized as a domestic or civil union partner under:

a. The provisions of any applicable federal, state, or local law; or

b. The provisions of any formal program established by "you".

19. **"Electronic Media Incident"** means an allegation that the display of information in electronic form by you on a website resulted in:

a. Infringement of another's copyright, title, slogan, trademark, trade name, trade dress, service mark, or service name;

b. Defamation against a person or organization that is unintended; or

c. A violation of a person's right of privacy, including false light and public disclosure of private facts.

20. **"Employee"** means any natural person, other than an "executive", who was, now is or will be:

a. Employed on a full-time or part-time basis by you;

b. Furnished temporarily to you to substitute for a permanent "employee" on leave or to meet seasonal or short-term workload conditions;

c. Leased to you by a labor leasing firm under an agreement between you and the labor leasing firm to perform duties related to the conduct of your business, but does not mean a temporary employee as defined in paragraph **b.**;

d. Your volunteer worker, which includes unpaid interns; or

e. An "independent contractor".

21. **"Executive"** means any natural person who was, now is, or will be:

a. The owner of your sole proprietorship; or

b. A duly elected or appointed:

1) Director;

2) Officer;

3) Managing Partner;

1) Other expenses that arise from the "computer fraud event";

2) Indirect loss, such as "bodily injury", lost time, lost wages, identity recovery expenses, or damaged reputation;

3) Any interest, time value, or potential investment gain on the amount of financial loss; or

4) Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.

8. **"Computer Fraud Event"** means:

a. An "unauthorized access incident" that leads to the intentional, unauthorized, and fraudulent entry of or change to data or instructions within a "computer system" owned or leased by you and operated under your control. Such fraudulent entry or change must be conducted by a person who is not an "employee", "executive", or "independent contractor". Such fraudulent entry or change must cause "money" to be sent or diverted. The fraudulent entry or change must result in direct financial loss to you.

b. "Computer fraud event" does not mean or include any occurrence:

1) In which you are threatened or coerced to send money or divert a payment; or

2) Arising from a dispute or a disagreement over the completeness, authenticity, or value of a product, a service, or a financial instrument.

9. **"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.

10. **"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".

11. **"Coverage Territory"** means:

a. With respect to Data Breach Response Expenses, Computer Attack, Cyber Extortion, Misdirected Payment Fraud, Computer Fraud, and Telecommunications Fraud, "coverage territory" means anywhere in the world.

b. With respect to Privacy Incident Liability, Network Security Liability, and Electronic Media 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.

12. **"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". This includes any payment made in the form of "money", "securities", cryptocurrency (including, but not limited to, Bitcoin, Ethereum and other forms of digital, virtual or electronic currency), or tangible goods. The payment of "cyber extortion expenses" must be approved in advance by us. We will not unreasonably withhold our approval. However, we may pay for "cyber extortion expenses" that were not approved in advance by us if we determine the following:

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.

At our sole discretion, we may choose to pay "cyber extortion expenses" in excess of the limit shown in the Declarations if doing so reduces the total amount of "loss" payable under this Cyber Risk Coverage.

13. **"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";

SECTION VII – CYBER SUITE COVERAGE 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 breach" 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, 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; or

      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. "Claim" includes a demand or proceeding arising from a "wrongful act" that is a "personal data breach" only when the "personal data breach" giving rise to the proceeding was covered under the Data Breach Response Expenses section of this Cyber Coverage, and you submitted a "claim" to us and provided notifications and services to "affected individuals" in consultation with us pursuant to Data Breach Response Expenses in connection with such "personal data breach".

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

7. **"Computer Fraud Costs"** means:

   a. The amount of "money" fraudulently obtained from you. "Computer fraud costs" include the direct financial loss only.

   b. "Computer fraud costs" do not include any of the following:

13. **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.

14. **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 may not be available or applicable to all individuals. 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.

15. **Transfer of Rights of Recovery Against Others To Us**

If the insured has rights to recover all or part of any payment we have made under this Cyber Coverage, those rights are transferred to us. The insured must do nothing after "loss" to impair them. At our request, the insured will bring "claim" or "suit" or transfer those rights to us and help us enforce them.

16. **Valuation**

We will determine the value of "money", "securities", cryptocurrency, and tangible property as follows:

a. Our payment for loss of "money" or loss payable in "money" will be, at your option, in the "money" of the country in which the "computer fraud event", "cyber extortion threat", "reward payments", or "wrongful transfer event" took place or in the United States of America dollar equivalent thereof determined at the rate of exchange published by the Wall Street Journal at the time of payment of such "loss".

b. Our payment for loss of "securities" will be their value at the close of business on the day the "computer fraud event" or the "wrongful transfer event" was discovered, or the day the "securities" were transferred by you in response to the "cyber extortion threat". At our option, we may:

1) Pay the value of such "securities" to you or replace them in kind, in which event you must assign to us all of your rights, title, and interest in those "securities"; or

2) Pay the cost of any Lost Securities Bond required in connection with issuing duplicates of the "securities"; provided that we will be liable only for the cost of the Lost Securities Bond as would be charged for a bond having a penalty not exceeding the lesser of the value of the "securities" at the close of business on the day the "computer fraud event", "cyber extortion threat", or "wrongful transfer event" was discovered.

c. Our payment of cryptocurrency will be its value at the close of business on the day the cryptocurrency was transferred by you in response to the covered "cyber extortion threat".

d. Our payment for the loss of tangible property will be the smallest of:

1) The cost to replace the tangible property; or

2) The amount you actually spend that is necessary to replace the tangible property.

We will not pay you on a replacement costs basis for any loss of tangible property until such property is actually replaced and unless the replacement is made as soon as reasonably possible after the "loss". If the lost property is not replaced as soon as reasonably possible after the "loss", we will pay you the actual cash value of the tangible property on the day the "computer fraud event", "cyber extortion threat", or "wrongful transfer event" was discovered.

2) Upon payment of the additional premium of 100% of the full annual premium associated with the relevant coverage, 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 before the end of the "policy period" 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, within thirty (30) days after the effective date of "termination of 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.

7. **Legal Action Against Us**

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

a. There has been full compliance with all of the terms of this insurance; and

b. The action is brought within two years after the date the "loss" is first discovered by you, or the date on which you first receive notice of a "claim" or "regulatory proceeding".

No person or organization has a right under this Cyber Coverage:

a. To join us as a party or otherwise bring us into a "suit" asking for damages from an insured; or

b. To sue us on this Cyber Coverage unless all of its terms have been fully complied with.

A person or organization may sue us to recover on an agreed settlement or on a final judgment against an insured; but we will not be liable for damages that are not payable under the terms of this Cyber Coverage or that are in excess of the applicable Limit of Insurance. An agreed settlement means a settlement and release of liability signed by us, the insured, and the claimant or the claimant's legal representative.

8. **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.

9. **Other Insurance**

If there is other insurance that applies to the same "loss", this Cyber Coverage shall apply only as excess insurance after all other applicable insurance has been exhausted.

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 Breach 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 breach" 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 Breach Response Expenses limit of insurance.

11. **Representations**

By accepting this Cyber Coverage, you agree:

a. The statements in the Declarations are accurate and complete;

b. Those statements are based upon representations you made us; and

We have issued this policy in reliance upon your representations.

12. **Separation of Insureds**

Except with respect to the Limits of Insurance, and any rights or duties specifically assigned in this Cyber Coverage to the first Named Insured, this insurance applies:

a. As if each Named Insured were the only Named Insured; and

b. Separately to each insured against whom "claim" is made or "suit" is brought.

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 practicable, but in no event more than sixty (60) days after the date the "claim" or "regulatory proceeding" is first received by you;

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 breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event" insured under this Cyber Coverage, you must see that the following are done:

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

2) Notify us as soon as practicable, but in no event more than sixty (60) days after the "personal data breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event". Include a description of any property involved.

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

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

a) Inspect the property proving the "personal data breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event";

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 breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event". You must do this within sixty (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 breach", "computer attack", "cyber extortion threat", "wrongful transfer event", or "computer fraud event".

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) Promptly 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 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.

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".

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 thirty (30) 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