MIIA Property and Casualty Group, Inc.
3 Center Plaza, Suite 610
Boston, MA 02108
www.emiia.org

MIIA Nonprofit Locally based Member driven
Serving Massachusetts communities since 1982

CYBER COVERAGE

MEMBER NAME AND ADDRESS **CONTRACT# EAS00488-03-23**

Town of East Bridgewater
175 Central Street
East Bridgewater, MA 02333

CONTRACT PERIOD **FROM 07/01/2023 TO 07/01/2024**

AT 12:01 AM STANDARD TIME
AT THE ADDRESS SHOWN ABOVE

SCHEDULE OF COVERAGES

Coverage	Limits of Insurance	Retentions, Waiting Periods, Period of Indemnity & Period of Restoration
1. Multimedia Liability	$1,000,000 each claim/aggregate	$10,000 each claim
2. Security and Privacy Liability	$1,000,000 each claim/aggregate	$10,000 each claim
3. Privacy Regulatory Defense and Penalties	$1,000,000 each claim/aggregate	$10,000 each claim
4. PCI DSS Liability	$1,000,000 each claim/aggregate	$10,000 each claim
5. Breach Event Costs	$1,000,000 each claim/aggregate	$10,000 each claim
Proactive Privacy Breach Event Costs Sublimit	$50,000 each claim/aggregate	$10,000 each claim
Voluntary Notification Expenses Sublimit	$1,000,000 each claim/aggregate	$10,000 each claim
6. BrandGuard	$1,000,000 each claim/aggregate	2 Week Waiting Period and 6 Month Period of Indemnity
7. Network Asset Protection	$1,000,000 each claim/aggregate	$10,000 each claim
Data Recovery		$10,000 each claim
Non-Physical Business Interruption		8 Hour Waiting Period and 6 Month Period of Restoration
8. Cyber Extortion	$100,000 each claim/aggregate	$10,000 each claim
9. Cyber Crime	$100,000 each claim/aggregate	$2,500 each claim
10. Dependent System Failure	$100,000 each claim/aggregate	12 Hour Waiting Period and 4 Month Period of Indemnity
11. Annual Aggregate Limit of Liability	$1,000,000	Not Applicable
12. Defense Costs Aggregate Limit	$1,000,000	Not Applicable

RETROACTIVE DATE 07/01/2019

FORMS AND ENDORSEMENTS ATTACHED TO THIS CONTRACT:

MDEC 3(0721), MCL 001(0722), MCL 003(0723)

CLAIM REPORTING: (800) 526-6442

WAR, CYBER WAR, AND CYBER OPERATIONS EXCLUSION ENDORSEMENT

THIS ENDORSEMENT CHANGES THE CONTRACT

This endorsement modifies coverage provided under the following:

CYBER COVERAGE FORM

This modifies and replaces Exclusion #29:

SECTION II - Exclusions

29. Notwithstanding any provisions to the contrary in this agreement or any endorsement thereto, this contract does not cover any loss, liability, damage, cost or expense of any kind (together "loss") directly or indirectly occasioned by, happening through or in consequence of:

a. "War"; or

b. a "Cyber Operation" that is carried out in the course of "War" (hereinafter Cyber War).

MIIA shall have the burden of proving that this exclusion applies.

Definitions:

"Cyber Operation" means the use of a "Computer System" by or on behalf of a sovereign state to disrupt, deny, degrade, manipulate or destroy information in a "Computer System" of or in another sovereign state.

"Computer System" means computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, and wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.

"War" means the use of physical force by a sovereign state against another sovereign state (whether war be declared or not) or as part of a civil war, rebellion, revolution, insurrection and/or military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority.

CYBER OPERATIONS EXCLUSION

Except as otherwise excluded under the War and Cyber War Exclusion, this contract does not cover any loss, damage, liability, cost or expense of any kind (together "loss") directly or indirectly occasioned by, happening through or in consequence of a "Cyber Operation" that has a major detrimental impact on: the functioning of a

sovereign state due to the direct or indirect effect of the "Cyber Operation" on the availability, integrity or delivery of an "essential service" in that sovereign state; and/or the security or defense of a sovereign state. However, this paragraph shall not apply to the direct or indirect effect of a "Cyber Operation" on a "Bystanding Cyber Asset".

MIIA shall have the burden of proving that this exclusion applies.

Attribution of a "Cyber Operation" to a sovereign state

For purposes of this exclusion, the primary but not exclusive factor in determining attribution of a "Cyber Operation" shall be whether the government of the sovereign state in which the "Computer System" affected by the "Cyber Operation" is physically located attributes the "Cyber Operation" to another sovereign state.

Pending attribution by the government of this sovereign state in which the "Computer System" affected by the "Cyber Operation" is physically located. It is agreed that during this period loss shall be paid by MIIA and all necessary adjustments subsequent to the payment of the loss shall be made by the parties hereto.

In the event that the government of the sovereign state in which the "Computer System" affected by the "Cyber Operation" is physically located either takes an unreasonable length of time to, or does not, or declares it is unable to attribute the "Cyber Operation" to another sovereign state, it shall be for MIIA to prove attribution by reference to such other evidence as is available.

Nothing in this clause shall be construed to mean that losses are not recoverable hereunder until MIIA's ultimate net loss has been ascertained.

Definitions

"Bystanding Cyber Asset" means a "Computer System" used by the insured or its third-party service providers that is not physically located in an "Impacted State" but is affected by a "Cyber Operation".

"Computer system" means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, and wearable device), server, could infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.

"Cyber Operation" means the use of a "Computer System" by or on behalf of a sovereign state to disrupt, deny, degrade, manipulate or destroy information in a "Computer System" of or in another sovereign state.

"Essential Service", for the purposes of this exclusion, means a service that is essential for the maintenance of vital functions of a sovereign state including without limitation: financial institutions and associated financial market infrastructure, emergency services, health services, utility services and/or services that are essential for the maintenance of the food, energy and/or transportation sector.

"Impacted State" means any sovereign state where a "Cyber Operation" has had a major detrimental impact on the functioning of that sovereign state due to the direct or indirect effect of the "Cyber Operation" on the availability, integrity or delivery of an "Essential Service" in that sovereign state; and/or the security or defense of that sovereign state.

"War" means the use of physical force by a sovereign state against another sovereign state (whether war be declared or not) or as part of a civil war, rebellion, revolution, insurrection, and/or military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority.