ARKANSAS INSURANCE DEPARTMENT
Risk Management Division
1 Commerce Way, Suite 504
Little Rock, Arkansas 72202
Phone: (501) 371-2690 Fax: (501) 371-2842
Email: *insurance.risk.management@arkansas.gov*
www.insurance.arkansas.gov

State of Arkansas Participating State Agency Entities

Cyber Liability Insurance Coverage Overview

2020-2021

This Cyber Liability Insurance Coverage Overview document does NOT convey or provide insurance coverage. Refer to the insurance policy for terms and conditions. See the master policy for specific policy limits and sub limits. Limits and retentions are subject to change upon renewal.

Section I – First Party Insuring Agreements

The Policy provides the **Insured** with coverage for loss as more fully and specifically described in the following Insuring Agreements:

A. **Cyber Incident Response Costs**

The Insurance Company will pay on behalf of the **Insured Cyber Incident Response Costs** up to the Limit of Liability and excess of the **Retention**, as stated in the Policy Schedule, arising out of an actual or suspected **Network security breach**, **Privacy breach** or a **Confidentiality breach** which first occurred on or after the **Retroactive Date** and was discovered during the **Policy Period**.

Cyber Incident Response Costs incurred consistent with the foregoing paragraph but after the period of time listed in the Policy Schedule and any **Cyber Incident Response Costs** incurred that do not utilize a vendor from the **Pre-Approved Providers from the Insurance Company Response Panel** are subject to **Insurance Company** prior written consent.

B. **Data Recovery Expenses**

C. **The Insurance Company** will pay the **Insured** for any **First Party Costs** up to the Limit of Liability and excess of the **Retention**, as stated in the Policy Schedule, for **Data Recovery Expenses** incurred as a direct result of damage to the **Insured's Data** or **Insured's Programs** caused by:

a. **Computer Attack**;
b. **Operational Error**;

which first occurred on or after the **Retroactive Date** and was **Discovered** during the **Policy Period.**

D. **Insured's Network Failure – Income Loss and Extra Expense**

The Insurance Company will pay the **Insured for** any **Income Loss** and **Extra Expense** up to the Limit of Liability as stated in the Policy Schedule, incurred by the **Insured** due to the suspension or deterioration of the **Insured's** business during the **Period of Restoration** directly as a result of the total or partial interruption, degradation in service or failure of the **Insured's Network**, provided that the duration of such interruption, degradation or failure exceeds the **Time Retention** and was directly caused by:

a. **Computer Attack**;
b. **Operational Error**;

which first occurred on or after the **Retroactive Date** and was **Discovered** during the **Policy Period.**

The Insurance Company will not be liable for any **Income Loss** and **Extra Expense** incurred during the **Time Retention**. The **Time Retention** will apply to each **Period of Restoration**.

E. **Outsource Service Provider or Cloud Service Provider Failure– Income Loss and Extra Expense**

The Insurance Company will pay the **Insured** for any **Income Loss** and **Extra Expense**, up to the Limit of Liability, as stated in the Policy Schedule, incurred by the **Insured** due to the suspension or deterioration of the **Insured's** Business during the **Period of Restoration** directly as a result of the total or partial interruption, degradation in service or failure of a **Network** operated by an **Outsource Service Provider** or **Cloud Service Provider** for the **Insured**, provided that the duration of such interruption, degradation or failure exceeds the **Time Retention** and was directly caused by:

a. **Computer Attack**;
b. **Operational Error**;

which first occurred on or after the **Retroactive Date** and was **Discovered** during the **Policy Period**.

The Insurance Company will not be liable for any **Income Loss** and **Extra Expense** incurred during the **Time Retention**. The **Time Retention** will apply to each **Period of Restoration**.

F. **Cyber Extortion and Ransomware**

The Insurance Company will reimburse the **Insured** for any **Cyber Extortion/Ransomware Payments** and any **Cyber Extortion/Ransomware Expenses** up to the Limit of Liability and excess of the **Retention**, as stated in the Policy Schedule, incurred directly as a result of a **Cyber Extortion Demand** or **Ransomware Demand** first made during the **Policy Period**.

G. **Customer Attrition**

The Insurance Company will pay the **Insured** for any **Customer Attrition Loss** and **Extra Expense** up to the Limit of Liability and excess of the Retention, as stated in the Policy Schedule, incurred by the **Insured** during the **Customer Attrition Period of Restoration** directly as a result of the reputational damage caused by an allegation made in the public domain or the release of information in the public domain to the effect that the **Insured** committed or failed to prevent a **Network Security Breach**, **Privacy Breach** or a **Confidentiality breach**, provided that such **Network Security Breach**, **Privacy Breach** or **Confidentiality Breach** first occurred on or after the **Retroactive Date** and was **Discovered** during the **Policy Period**.

H. **Hardware**

The Insurance Company will reimburse the insured for the replacement of any hardware under the insured's direct ownership and operation that is deemed unfit for purpose, up to the limit of liability and excess of the **retention** as stated in the policy schedule, occurring as a direct result of a network security breach on the insured's network, which occurred on or after the retroactive date and which was discovered during the policy period.

Section II – Third Party Insuring Agreements

The Policy provides the **Insured** with coverage for **Claims** made under the following Insuring Agreements, as more fully described below:

I. **Network Security, Privacy and Confidentiality Liability**

The Insurance Company will pay on behalf of the **Insured** any **Damages** and **Defense Costs** up to the Limit of Liability and excess of the **Retention**, as stated in the Policy Schedule, arising out of a **Claim** first made against the **Insured** during the **Policy Period** alleging that the **Insured** committed or failed to prevent a **Network Security Breach**, **Privacy breach** or a **Confidentiality breach** which first occurred on or after the **Retroactive Date**.

J. **Network Security and Privacy Liability (Regulatory Penalties and Investigation Costs)**

The Insurance Company will pay on behalf of the **Insured** any **Regulatory Penalties** and **Regulatory Investigation Costs** up to the Limit of Liability and excess of the **Retention**, as stated in the Policy Schedule, arising out of a **Regulatory Claim** first made against the **Insured** during the **Policy Period** alleging that the **Insured** committed or failed to prevent a **Network Security Breach**, **Privacy Breach** or a **Confidentiality Breach** which first occurred on or after the **Retroactive Date**.

K. **Multimedia Liability**

The Insurance Company will pay on behalf of the **Insured** any **Damages** and **Defense Costs** up to the Limit of Liability and excess of the **Retention**, as stated in the Policy Schedule, arising out of a **Claim** first made against the **Insured** during the **Policy Period** alleging that the **Insured** committed, either directly or indirectly, or failed to prevent a **Multimedia Wrongful Act** which first occurred on or after the **Retroactive Date**.

L. **Technology Errors and Omissions**

The Insurance Company will pay on behalf of the **Insured** any **Damages** and **Defense Costs** up to the Limit of Liability and excess of the **Retention**, as stated in the Policy Schedule, arising out of a **Claim** first made against the **Insured** during the **Policy Period** alleging that the **Insured** committed a **Technology Error and Omission** which first occurred on or after the **Retroactive Date**.

Section III – Payment Card Industry Data Security: Fines, Penalties and Assessments

M. **Payment Card Industry Data Security Standard (hereinafter "PCI DSS"): Fines, Penalties and Assessments**

The Insurance Company will pay on behalf of the **Insured** any **PCI DSS Fines, Penalties and Assessments** and **PCI DSS Claim Expenses** up to the Limit of Liability and excess of the **Retention**, as stated in the Policy Schedule, arising out of a **PCI DSS Claim** first made against the **Insured** during the **Policy Period** alleging that the **Insured** committed or failed to prevent a **Network Security Breach**, **Privacy Breach** or a **Confidentiality Breach** which first occurred on or after the **Retroactive Date**.

Section IV – Cyber Terrorism

N. **Cyber Terrorism**

If a loss or **Claim** is covered under one or more of the Insuring Agreements listed above, coverage will still be provided under that Insuring Agreement(s) in the event of a **Cyber Terrorism Event.**, but only if this Section IV is marked as applicable in the Policy Schedule. No Limits of Liability are provided by this Policy Section in addition to the Limits of Liability already provided by the specific Insuring Agreements.

DEFINITIONS

Cyber Incident Response Costs mean:

a. Costs to notify the population impacted or potentially impacted by a breach (including but not limited to call center costs in handling calls from notified individuals), reasonably and necessarily incurred by the **Insured** as a result of a legal or regulatory requirement including but not limited to legal, postage, advertising (not including public relations consultants) and other related expenses. This shall specifically include legal expense and other costs incurred to determine whether a suspected breach is in fact a breach.
b. Where there is no legal or regulatory requirement to notify the population impacted or potentially impacted by a breach or suspected breach, costs to notify, including but not limited to postage, advertising and other related expenses, including legal expenses incurred after it is determined that there is no legal or regulatory requirement to notify, will only be considered by **The Insurance Company** under the following circumstances and subject to **The Insurance Company** prior written consent: i) such costs are intended to mitigate further loss or a **Claim** or potential claim that is covered under this Policy; ii) where the **Insured** has received legal advice recommending that there is a legal or regulatory requirement to notify other portions of the breached population for the same breach or suspected breach; or iii) where the **Insured** has received legal advice that such costs are necessary to

mitigate reputational damage to the **Insured**.

c. Costs to provide credit monitoring and/or identity theft assistance solutions to the population impacted or potentially impacted by a breach for a period as legally required up to a maximum of 2 years, reasonably and necessarily incurred by the **Insured**, including but not limited to credit file monitoring and protection, purchase of identity theft insurance and consultation services.
d. Costs to appoint a public relations consultant, being all public relations consultancy fees reasonably and necessarily incurred by the **Insured** in mitigating the reputational damage caused by a **Network Security Breach**, **Privacy Breach**, or a **Confidentiality Breach**.
e. Forensics expenses, being all reasonable and necessary costs that the **Insured** incurs for the purposes of conducting a review or investigation of the source or cause of an actual or suspected **Network Security Breach**.

Computer Attack means a denial of service attack, use of malicious code/malware, computer virus or any other unauthorized use of the **Insured's Network** (including use by an authorized person(s) for an unauthorized purpose), which is either intended to cause damage to the **Insured's** N**etwork**, or as a result of an attack elsewhere, causes damage to the **Insured's Network**.

Confidentiality Breach means:

a. The breach of any legal, regulatory or contractual requirement to protect the security or confidentiality of non-public corporate or other business confidential information, including but not limited to business plans and forecasting information, valuations, product development, banking and tax practice.
b. The failure to destroy non-public corporate or other business confidential information including but not limited to business plans and forecasting information, valuations, product development, banking and tax practice, which breaches a legal, regulatory or contractual requirement.

Network Security Breach means:

a. The malicious or unauthorized takeover or use of the **Insured's Network**, which either directly or indirectly results in or contributes to the:
    i. damage, modification, theft, corruption, distortion, copy, deletion, misuse or destruction of **Data**, **Programs** or **Networks**.
    ii. launch of a denial of service attack or failure to prevent or hinder such attack.
    iii. transmission of malicious code from the **Insured's Network** to a **Third-Party Network**
    or failure to prevent or hinder such transmission.
b. A phishing, pharming, spoofing or any other attack designed similarly to steal personally identifiable information, protected health information or non-public corporate or other business confidential information including but not limited to bank details.
c. The breach of the **Insured's** network security policy.

Operational Error means the unintentional, accidental, negligent act, error or omission in entering or modifying the **Insured's Data** (including the damage or deletion thereof), or in

creating, handling, developing, modifying, or maintaining the **Insured's Data** or **Programs**, or in the ongoing operation or maintenance of the **Insured's Network**.

Personal Identifiable Non-Public Information means:

a. Information concerning the individual that constitutes "non-public personal information" as defined in the Gramm-Leach Bliley Act of 1999, as amended, and regulations issued pursuant to the Act or any similar laws, rules, or regulations in other jurisdictions, including foreign jurisdictions;
b. medical or healthcare information concerning the individual, including "protected health information" as defined in the Health Insurance Portability and Accountability Act of 1996, as amended, and regulations issued pursuant to the Act, or any similar laws, rules or regulations in other jurisdictions, including foreign jurisdictions;
c. information concerning the individual that is defined as private personal information in any statute, law or regulation that requires notice to persons whose private personal information was accessed or reasonably may have been accessed by an unauthorized person, entity, or program;
d. Information concerning the individual that is defined as private personal information under statutes or laws enacted to protect such information in foreign countries, for **Claims** or losses subject to the law of such jurisdiction;
e. the individual's drivers license or state identification number; social security number; unpublished telephone number; and credit, debit or other financial account numbers in combination with associated security codes, access codes, passwords or PINs; if such information allows an individual to be uniquely and reliably identified or contacted or allows access to the individual's financial account or medical record information but does not include publicly available information that is lawfully made available to the general public from government records.

Privacy Breach means:

a. The unauthorized acquisition, access, use, or disclosure of **Personal Identifiable Non-Public Information,** which compromises the security or privacy of such information and breaches a legal, regulatory or contractual requirement to protect the security or confidentiality of this information;
b. Failure to comply with any applicable law, regulation or contractual requirement requiring the disclosure of what is enumerated in "a" above;
c. The wrongful collection of **Personal Identifiable Non-Public Information**, which breaches a legal, regulatory or contractual restriction;
d. The failure to destroy **Personal Identifiable Non-Public Information,** which breaches a legal, regulatory or contractual restriction;
e. The breach of privacy rights or any similar or equivalent allegation in the jurisdiction in which the **Claim** is brought; or
f. The breach of the **Insured's** privacy policy.

Retroactive Date means the date specified in the Policy Schedule.