NAPA Premier

Please complete the form and email Jon Talamas at
Jon_Talamas@ajg.com or Joe Peters at **Joe_Peters@ajg.com**

Cyber Liability And Privacy Coverage Application

94.001-4 (03/21)

CERTAIN COVERAGES OFFERED ARE LIMITED TO LIABILITY FOR CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED AND NOTIFIED TO US DURING THE POLICY PERIOD AS REQUIRED. CLAIM EXPENSES SHALL REDUCE THE APPLICABLE LIMITS OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION(S). PLEASE READ THE POLICY CAREFULLY.

"You", "Your Organization", and "Applicant" mean all corporations, organizations or other entities, including subsidiaries, proposed for this insurance.

I. GENERAL INFORMATION

Name of Applicant	
Mailing Address	
City	
State	
ZIP Code	
Description of Applicant's Operations	
Applicant Contact Name	
Applicant Contact Email Address	
Applicant Website	
Custodian	

II. REVENUES

Indicate the following as it relates to the Applicant's fiscal year end (FYE):	**Prior FYE**
Gross Fees	$

III. NETWORK SECURITY SYSTEM

1. a. Do "You", or an outsourced firm, back up your data and systems at least once a week, and store these backups in an offsite location?	Yes ☐	No ☐
b. If yes, can "You" recover all of your business-critical data and systems within 10 days?	Yes ☐	No ☐
2. Do "You" have anti-virus software and firewalls in place that are regularly updated (at least quarterly)?	Yes ☐	No ☐

3. a. Do "You" have Remote Desktop Protocol (RDP) (or any other type of remote access to desktops or servers or applications) enabled? Yes ☐ No ☐

   b. If yes, do "You" utilize Multi-Factor Authentication (MFA) when accessing all desktops or servers or applications remotely? Yes ☐ No ☐

4. After inquiry of the "Control Group", as defined, are "You" aware of any or have any grounds for suspecting any circumstances which might give rise to a claim? Yes ☐ No ☐

5. Within the last 5 years, has "Your Organization" suffered any system intrusions, tampering, virus or malicious code attacks, loss of data, loss of portable media, hacking incidents, extortion attempts, or data theft, resulting in a claim in excess of $25,000 that would be covered by this insurance? Yes ☐ No ☐

If the "Applicant" represents a Healthcare organization, Financial Institution or Legal Services (consumer) then the following question MUST be answered:

6. Do "You" have a written policy which requires that personally identifiable information stored on mobile devices (e.g. laptop computers / smartphones) and portable media (e.g. flash drives, back-up tapes) be protected by encryption? Yes ☐ No ☐

* With respect to the information required to be disclosed in response to the questions above, the proposed insurance will not afford coverage for any claim arising from any fact, circumstance, situation, event or act about which any member of the "Control Group" of the "Applicant" had knowledge prior to the issuance of the proposed policy, nor for any person or entity who knew of such fact, circumstance, situation, event or act prior to the issuance of the proposed policy.

"Control Group" means:
The board members, executive officers, Chief Technology Officer, Chief Information Officer, Risk Manager and General Counsel or their functional equivalents of "Your Organization". This does not include any administrative staff who work in the offices of these named positions.

IV. CYBER DECEPTION (inc. Social Engineering coverage)

1. Does the "Applicant" have procedures in place requiring two people, processes, or devices to verify any changes in transfer details and obtain authorization when transferring funds in excess of $10,000 to external parties? Yes ☐ No ☐

2. Does the **Applicant** provide training for staff members who transact funds in excess of $10,000 externally? Yes ☐ No ☐

3. Does the Applicant have a call-back verification process when making changes to or setting up new payment instructions to a third party? Yes ☐ No ☐

4. Have there been any losses for a "Cyber Deception Event" in the past year in excess of $10,000? Yes ☐ No ☐

5. After inquiry of the "Control Group", as defined, have there been any claims or circumstances arising from "Cyber Deception Events" which may give rise to a claim that could be covered by the Cyber Deception coverage being applied for? Yes ☐ No ☐

Please note that the Cyber Deception Coverage applied will not attach to those matters identified above that are claims or may be reasonably expected to give rise to a claim, under the Cyber Deception Coverage.
"Cyber Deception Event" means:

1. The good faith transfer by "You" of "Your Organization's" funds or the transfer of "Your Goods", in lieu of payment, to a third party as a direct result of a "Cyber Deception", whereby "You" were directed to transfer "Goods" or pay funds to a third party under false pretences; or
2. The theft of "Your Organization's" funds as a result of an unauthorized intrusion into or "Security Compromise" of "Your" "Computer System" directly enabled as a result of a "Cyber Deception".

"Control Group" means:
The board members, executive officers, Chief Technology Officer, Chief Information Officer, Risk Manager and General Counsel or their functional equivalents of “Your Organization”. This does not include any administrative staff who work in the offices of these named positions.

REQUIRED FRAUD WARNING LANGUAGE:

It is a crime to knowingly and intentionally attempt to defraud an insurance company by providing false or misleading information or concealing material information during the application process or when filing a claim. Such conduct could result in your policy being voided and subject you to criminal and civil penalties.

Signature of Applicant’s Authorized Representative

Name (Printed)

Title

Date