BCS INSURANCE COMPANY
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181

Cyber Liability And Privacy Coverage Application

94.001-3 (09/15)

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 Company, 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	

II. INSURANCE TERMS/CURRENT INSURANCE INFORMATION

The following table details the limits and retentions being offered:

Insuring Agreement	Limit	Retention
A. Privacy Liability	$1,000,000	
B. Privacy Regulatory Claims Coverage	$1,000,000	
C. Security Breach Response Coverage	$1,000,000	
D. Security Liability	$1,000,000	
E. Multimedia Liability	$1,000,000	
F. Cyber Extortion	$1,000,000	
G. Business Income and Digital Asset Restoration	$1,000,000	
H. PCI DSS Assessment	$100,000	

III. REVENUES

Indicate the following as it relates to the Applicant's fiscal year end (FYE):	**Prior FYE**
Total Revenue	

IV. NETWORK SECURITY

SYSTEMS

1. 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 ☐
2. Do **You** have anti-virus software and firewalls in place that are regularly updated (at least quarterly)? Yes ☐ No ☐
3. Are **You** aware of any or have any grounds for suspecting any circumstances which might give rise to a claim? Yes ☐ No ☐
4. Within the last 5 years, has **Your Company** 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** is a Healthcare organization, Financial Institution or Legal Services (consumer) then the following question MUST be answered:

5. 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 executive officer 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.

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 (President, CEO or Chief Information/Security Officer)

Name (Printed)

Title

Date

CYBER DECEPTION SUPPLEMENTAL APPLICATION

1.	Does the **Applicant** have dual control when transferring funds in excess of $25,000 to external parties?	Yes ☐	No ☐
2.	Does the **Applicant** provide training for staff members who transact funds in excess of $25,000 externally	Yes ☐	No ☐
3.	Have there been any losses for a "Cyber Deception Event" in the past year in excess of $10,000?	Yes ☐	No ☐

"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".

Signature * of Applicant's Authorized Representative Name (Printed) (President, CEO or Chief Information/Security Officer)

Name (Printed)

Title

Date