

**APPLICATION FOR ARCH NETSAFESM**

**ENTERPRISE NETWORK AND PRIVACY INSURANCE**

This is an application for **CLAIMS MADE AND REPORTED INSURANCE.** Such insurance, if accepted by the Company, applies only to claims first made against the Insured and reported to the Company during the Policy Period, unless an extended reporting period applies. Refer to terms and conditions of the policy for coverage limitations.

**NOTICE: THE LIMIT OF LIABILITY IN THE POLICY, IF ISSUED, MAY BE REDUCED OR COMPLETELY EXHAUSTED BY CLAIM COST AND/OR LEGAL DEFENSE. IN SUCH EVENT, THE COMPANY SHALL NOT BE LIABLE FOR ANY JUDGMENT, SETTLEMENT OR CLAIM COST OR LEGAL DEFENSE COST WHICH ARE IN EXCESS OF THE LIMITS OF LIABILITY STATED ON THE DECLARATIONS PAGE OF POLICY.**

**THE DEDUCTIBLE IN THE POLICY, IF ISSUED, APPLIES TO CLAIM COSTS AND LEGAL DEFENSE AS WELL AS TO JUDGMENTS AND SETTLEMENTS.**

Instructions to the Applicant:

- Please answer all the questions. The information is required to make an underwriting and pricing
 evaluation. Your answers hereunder are considered legally material to the evaluation.

- If a question is not applicable, state N/A. If more space is required to answer a question, please
 attach an exhibit with question number.

1. Name of Applicant Firm:

 Website Addresses:

2. Home Office Address:

3. Locations of all branch offices:

1. Names and locations of all subsidiaries or affiliates for which coverage is desired:

**Financial Information and details of services offered:**

Total Revenue for the Past 12 Months:

Projected Revenue for the Next 12 Months:

Percent of Revenues Network Dependent:

**If Errors & Omissions/Professional Liability is required, please complete the supplemental application**.

**General Information:**

Provide a brief description of your business operations:

Company Formation Date:

Total Number of Employees in the Company:

Number of Locations where Servers are Located:

1. In the next 12 months will you accept, store, process, or exchange credit/debit card transaction information?

Yes [ ]  No [ ]

**If yes:**

* 1. For PCI compliance, applicant is considered Service Provider or Merchant Level: I [ ]  II [ ]  III [ ]  IV [ ]
	2. Have you had a PCI compliance audit performed in the last 12 months by an approved PCI Qualified Security Assessor? Yes [ ]  No [ ]
	3. If Yes, have you been certified as fully PCI compliant? Yes [ ]  No [ ]  Date:

If No, please provide an explanation:

* 1. Approximately how many credit/debit card transactions do you expect to handle in the next 12 months companywide:
1. Please identify the private information being handled, including that of your own employees (check all that apply and provide the approximate number of records):

[ ]  Social security number \_\_\_\_\_\_\_\_\_\_\_\_

[ ]  Drivers license number or any other state identification number \_\_\_\_\_\_\_\_\_\_

[ ]  Medical or healthcare data including protected health information\_\_\_\_\_\_\_\_\_\_

[ ]  Any account number, credit or debit card number in combination with any required password,

access code, or other security code that would permit access to the financial account \_\_\_\_\_\_\_\_

[ ]  Proprietary business information\_\_\_\_\_\_\_\_\_\_

[ ]  3rd Party confidential information\_\_\_\_\_\_\_\_

1. For the private information collected, is there a process for deleting this information once it is complete or not needed anymore? Yes [ ]  No [ ]
2. Are you compliant with the following (if No, please explain on a separate sheet):
	1. Health Insurance Portability and Accountability Act (HIPAA) Yes [ ]  No [ ]  NA [ ]
	2. Gramm-Leach Bliley Act of 1999 (GLBA) Yes [ ]  No [ ]  NA [ ]
3. For HIPAA, GLBA and/or other state or federal regulation compliance, what due diligence/auditing is performed to ensure that you remain in compliance and what individual(s) in your organization are responsible for said compliance?

**Media Controls:**

1. Do you provide legal, financial, medical and/or health advice on your website? Yes [ ]  No [ ]  NA [ ]
2. Do you provide personal finance or other personal advice services, such as counseling on your website?

Yes [ ]  No [ ]  NA [ ]

1. Do you publish a bulletin board, chat room or otherwise allow users to upload or post content to your website?

Yes [ ]  No [ ]

 If yes, do you have a process for monitoring, approving and removing such content? Yes [ ]  No [ ]

1. Do you have legal review of your website(s) performed by staff or outside attorney? Yes [ ]  No [ ]  If, no, what review is being completed? ­­­­­­­­­­­­­­­­
2. Is legal review performed on all intellectual property utilized in the course of your business operations?

 Yes [ ]  No [ ]  NA [ ]

If no, please explain:

**Network Security & Employee Controls**

**If you answer NO to any of the questions below please explain in a separate attachment.**

1. Check all that apply and name the service provider for each category (please attach the representative contract/agreement):
	1. Hosting Facility [ ]
	2. Co-location Facility [ ]
	3. Managed Security Service Provider (MSSP) [ ]
	4. Application Service Provider (ASP) [ ]
	5. Data Storage Facility [ ]
	6. Payroll[ ]
	7. Benefits[ ]
	8. Other Human resource functions[ ]
	9. Other (please specify) [ ]
2. Do you have any data sharing agreements with any 3rd parties? Yes [ ]  No [ ]  (Please provide details)

a) Do you have contracts in place with the 3rd parties that require the vendor to maintain controls, practices and procedures that are as protective as your own internal procedures? Yes [ ]  No [ ]

b) Do the contracts require the 3rd parties to defend and indemnify you for liability arising from their use of the data they are handling? Yes [ ]  No [ ]

1. Do you regularly audit 3rd parties with whom you have data sharing agreements with? Yes [ ]  No [ ]
	1. If No, how do you ensure their compliance with HIPAA, PCI, etc.?
2. Does your company have a current information security policy that has been approved by executive management? Yes [ ]  No [ ]
	1. If Yes, does the policy specify acceptable use of all company resources including the proper use of email and the Internet? Yes [ ]  No [ ]
	2. If Yes, are all employees provided with a copy of the policy? Yes [ ]  No [ ]
	3. If Yes, area all employees required to provide written confirmation they have read and understood the contents of the policy? Yes [ ]  No [ ]
3. Is there an information classification program that specifies different levels of security based on the nature of a given information asset? Yes [ ]  No [ ]

a. If Yes, are user accounts audited regularly to determine their security levels are appropriately set?

 Yes [ ]  No [ ]

1. Does your company have an information security officer? Yes [ ]  No [ ]
2. Are documented procedures in place for user and password management and are they monitored for compliance? Yes [ ]  No [ ] Do you have a process for managing user accounts including promptly deleting or modifying access upon a change of responsibilities or termination? Yes [ ]  No [ ]
3. Are special privileges restricted to systems administration personnel with an approved need to have these privileges? Yes [ ]  No [ ]
	1. Provide a brief description of the measures taken to ensure the physical security of computer systems from

 unauthorized entry/access.

1. Is there a patch management process in place? Yes [ ]  No [ ]  If, yes, what is the timeframe for implementing patches following identification?
2. Is firewall technology used to prevent unauthorized access to and from internal networks and external networks?

Yes [ ]  No [ ]

a. Are firewall configurations regularly reviewed and kept up to date? Yes [ ]  No [ ]

1. Is anti-virus software installed on all computers/servers that connect to your network? Yes [ ]  No [ ]
	1. Is the anti-virus software package updated regularly? Yes [ ]  No [ ]  How often?
	2. Are the virus signature files updated daily (or in close step with updates provided by the software

company)? Yes [ ]  No [ ]

* 1. Is there an appropriately trained security analyst on staff to assist in identifying and mitigating incidents involving undetected malware? Yes [ ]  No [ ]
	2. Are systems regularly audited to identify inappropriate code and/or applications that have been installed? Yes [ ]  No [ ]
1. Are system backup and recovery procedures documented and regularly tested for all mission critical systems/websites? Yes [ ]  No [ ]  If no, how often?
2. Do you allow remote access to your system? Yes [ ]  No [ ]  If yes, what controls are in place to prevent unauthorized access?
3. Are network and system backups performed at least once per week? Yes [ ]  No [ ]
4. Do you or any third parties conduct any penetration & vulnerability testing? Yes [ ]  No [ ]  If yes, have any major findings been remediated?       If not, please explain.
5. Do you monitor security alerts and advisories from your system vendors, Computer Emergency Response Team (CERT) and other sources, taking appropriate and responsive actions? Yes [ ]  No [ ]
6. Do you monitor your network in real time to detect possible intrusions or abnormalities in the performance of your system? Yes [ ]  No [ ]  If no, please explain how you monitor your network.
7. Do you monitor log files on a regular basis to help spot abnormal trends? Yes [ ]  No [ ]  For how long are log files maintained?
8. Are there redundant connections to you critical business partners? Yes [ ]  No [ ]
9. Do you have a written business continuity/disaster recovery plan that includes procedures to be followed in the event of a disruptive computer incident? Yes [ ]  No [ ]
10. Is your security policy reviewed and updated at least annually? Yes [ ]  No [ ]
11. Does your hiring process include the following (check all that are applicable):

All Employees Some Employees Ind. Cont. Not Required

Criminal Background Check [ ]  [ ]  [ ]  [ ]

Drug Tests [ ]  [ ]  [ ]  [ ]

Work History Verification [ ]  [ ]  [ ]  [ ]

Educational Verification [ ]  [ ]  [ ]  [ ]

Credit Check [ ]  [ ]  [ ]  [ ]

If checks only required in some circumstances but not others, please explain.

22. In the past 12 months, have you recently had layoffs or do you anticipate layoffs in the coming 12 months?

Yes [ ]  No [ ]  (if Yes, please explain)

**PRIVACY CONTROLS**

1. Do you have a dedicated Privacy officer **?** Yes [ ]  No [ ]
2. Do you have a privacy policy? Yes [ ]  No [ ]
3. Is your privacy policy posted on your website and made available to your customers prior to them providing personal information? Yes [ ]  No [ ]
4. Is your privacy policy reviewed and updated at least annually? Yes [ ]  No [ ]
5. Do you sell or share the personal subscriber/customer information with other unaffiliated 3rd parties? Yes [ ]  No [ ]

a) If Yes, do you provide opt-out controls that are visible and addressed within the privacy policy? Yes [ ]  No [ ]

b) Do you notify customers upon the release of their private information? Yes [ ]  No [ ]

1. Do you train employees on the proper handling of private information? Yes [ ]  No [ ]
2. Do you utilize retained private information in any other way than originally intended or disclosed? Yes [ ]  No [ ]

a) If yes, please explain:

1. Do you have a document retention and destruction policy? Yes [ ]  No [ ]  (Please expound)

1. Do you have policies/procedures in place for handling employees that are terminated or leave voluntarily?

Yes [ ]  No [ ]

* 1. Does the policy specifically address their access to corporate applications and personal information including proprietary corporate information? Yes [ ]  No [ ]
1. Do you conduct an annual privacy assessment to ensure that you are in compliance with privacy laws and regulations? Yes [ ]  No [ ]  If No, Please explain*:*

1. Are procedures in place to escalate any incidents of a breach or possible breach of private information? Yes [ ]  No [ ]
2. Do you ensure that all private information is encrypted whether at rest or in transit? Yes [ ]  No [ ]
	1. If not technically feasible, what safeguards are in place to ensure the security of private information?
	2. If Data and/or Private Information is not in electronic form, what precautions are taken to ensure its security?
3. Is data (i.e. personal information) encrypted on laptops and other mobile devises used for storing and transferring data? Yes [ ]  No [ ]
4. Do you allow sensitive data to be loaded on to devices that may be removed from the premises? Yes [ ]  No [ ]

**Prior Losses, Circumstances, & Events (Required for All Applicants):**

**IF YOU ANSWER YES TO ANY OF THESE QUESTIONS PLEASE ATTACH SEPARATE SHEET(S) WITH A FULL DESCRIPTION OF EACH INCLUDING DATES, ALLEGATIONS, CIRCUMSTANCES, COSTS, SETTLEMENT/JUDGEMENT AMOUNTS, ETC.**

1. During the last 3 years, have you had any information security breaches including unauthorized access, unauthorized use, virus, denial of service attack, breach, theft of data, fraud, electronic vandalism, sabotage or other security events. Yes [ ]  No [ ]
2. During the last 3 years, has anyone alleged that you were responsible for damages to their systems arising out of the operation of your system? Yes [ ]  No [ ]
3. During the last 3 years, have you received a complaint or an injunction arising out of intellectual property infringement, content or advertising? Yes [ ]  No [ ]
4. During the last 3 years, has anyone made a demand, claim, complaint, or filed a lawsuit against you that would or could be covered under this policy? Yes [ ]  No [ ]
5. During the last 3 years, have you been the subject of an investigation or action by any regulatory or administrative agency for privacy related violations? Yes [ ]  No [ ]
6. Has any application for similar insurance been declined or has any such insurance ever been rescinded, cancelled or been refused renewal? Yes [ ]  No [ ]
7. During the last 3 years, have you experienced a disruption to your computer system that lasted longer than 4 hours for any reason (other than planned downtime)? Yes [ ]  No [ ]
8. Are you aware of any circumstance or event that could result in a claim being made against the policy being applied for? Yes [ ]  No [ ]

**PLEASE ATTACH THE FOLLOWING:**

Errors & Omissions supplemental if such coverage is desired:

1. Please include a standard contract representative of the services provided including promotional

 material

Copy of standard contract used with service providers.

Privacy Policy.

Data Sharing Agreements

Copy of an Organization Chart.

 Copy of the Most Current Audited Financial Statements.

**APPLICATION MUST BE SIGNED AND DATED BY AN AUTHORIZED OFFICER, PARTNER OR PRINCIPAL.**

THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE COMPANY, NOR DOES IT OBLIGATE THE COMPANY TO ISSUE A POLICY OR INSURE ANY SERVICES. HOWEVER, IT IS AGREED THAT SHOULD A POLICY BE ISSUED, THIS APPLICATION WILL BE ATTACHED TO AND MADE A PART OF THE POLICY.

**THE UNDERSIGNED(S) CERTIFIES THAT HE/SHE IS THE DULY AUTHORIZED REPRESENTATIVE(S) OF EACH PROPOSED INSURED WHICH SUBMITS THIS APPLICATION TO THE ARCH SPECIALTY INSURANCE COMPANY FOR A POLICY OF INSURANCE. THE STATEMENTS AND INFORMATION ABOVE AND ALL SCHEDULES AND DOCUMENTS SUBMITTED, OF WHICH THE UNDERWRITER RECEIVES NOTICE, ARE DEEMED PARTS OF THE APPLICATION (ALL OF WHICH SCHEDULES AND DOCUMENTS SHALL BE DEEMED ATTACHED TO THE POLICY AS IF PHYSICALLY ATTACHED THERETO), AND THE WORD "APPLICATION" REFERS TO ALL OF THE FOREGOING.**

**EACH PROPOSED INSURED REPRESENTS THAT THE STATEMENTS SET FORTH IN THE APPLICATION ARE TRUE AND CORRECT, AND THAT REASONABLE EFFORTS HAVE BEEN MADE TO OBTAIN INFORMATION SUFFICIENT FOR ACCURATE COMPLETION OF THIS APPLICATION. IT IS FURTHER AGREED BY EACH PROPOSED INSURED THAT EACH POLICY OR RENEWAL THEREOF, IF ISSUED, IS ISSUED IN RELIANCE UPON THE TRUTH OF THE REPRESENTATIONS AND INFORMATION IN THE APPLICATION.**

**EACH PROPOSED INSURED UNDERSTANDS AND AGREES THAT ANY INSURANCE POLICY ISSUED BY THE COMPANY SHALL BE SUBJECT TO RESCISSION IF THIS APPLICATION CONTAINS ONE OR MORE MISREPRESENTATIONS OR OMISSIONS MATERIAL TO THE ACCEPTANCE OF THE RISK BY THE COMPANY.**

**IF THE INFORMATION SUPPLIED ON THIS APPLICATION OR ATTACHMENTS THERETO CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE INCEPTION DATE OF THE POLICY, THE APPLICANT WILL IMMEDIATELY NOTIFY THE COMPANY OF SUCH CHANGES.**

**NOTICE: ANY PERSON WHO, KNOWINGLY OR WITH INTENT TO DEFRAUD OR TO FACILITATE A FRAUD AGAINST ANY INSURANCE COMPANY OR OTHER PERSON, SUBMITS AN APPLICATION OR FILES A CLAIM FOR INSURANCE CONTAINING FALSE, DECEPTIVE OR MISLEADING INFORMATION MAY BE GUILTY OF INSURANCE FRAUD.**

**NOTICE TO ARKANSAS, LOUISIANA AND NEW MEXICO APPLICANTS:** Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit, or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

**NOTICE TO COLORADO APPLICANTS:** It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an Insurance Company for the purpose of defrauding or attempting to defraud the Company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any Insurance Company or agent of an Insurance Company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

**NOTICE TO DISTRICT OF COLUMBIA APPLICANTS:** Warning: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the applicant.

**NOTICE TO FLORIDA APPLICANTS:** Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete or misleading information is guilty of a felony in the third degree.

**NOTICE TO KENTUCKY APPLICANTS:** Any person who knowingly and with the intent to defraud any Insurance Company or other person files an application for insurance containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

**NOTICE TO MAINE APPLICANTS:** It is a crime to provide false, incomplete or misleading information to an Insurance Company for the purpose of defrauding the Company. Penalties may include imprisonment, fines or a denial of insurance benefits.

**NOTICE TO NEW JERSEY APPLICANTS:** Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

**NOTICE TO NEW YORK APPLICANTS:** Any person who knowingly and with intent to defraud any Insurance Company or other person files an application for insurance or statement of claims containing any materially false information, or conceals for the purpose of misleading information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

**NOTICE TO OHIO APPLICANTS:** Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

**NOTICE TO OKLAHOMA APPLICANTS:** WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony

**NOTICE TO PENNSYLVANIA APPLICANTS:** Any person who knowingly and with the intent to defraud any Insurance Company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

**NOTICE TO PUERTO RICO APPLICANTS**: Any person who knowingly and with the intent to defraud, presents false information in an insurance request form, or who presents, helps, or has presented a fraudulent claim for the payment of a loss or other benefit, or presents more than one claim for the same damage or loss, will incur a felony, and upon conviction will be penalized for each violation with a fine of no less than five thousand dollars ($5,000) nor more than ten thousand dollars ($10,000); or imprisonment for a fixed term of three (3) years, or both penalties. If aggravated circumstances prevail, the fixed established imprisonment may be increased to a maximum of five (5) years; if attenuating circumstances prevail, it may be reduced to a minimum of two (2) years.

**NOTICE TO TENNESSEE & VIRGINIA APPLICANTS:** It is a crime to knowingly provide false, incomplete or misleading information to an Insurance Company for the purpose of defrauding the Company. Penalties include imprisonment, fines and denial of insurance benefits.

**NOTICE TO WASHINGTON APPLICANTS:** It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines, and denial of insurance benefits.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**SIGNED BY AUTHORIZED OFFICER, PARTNER OR PRINCIPAL**

**PRINT OR TYPE NAME & TITLE**

**PHONE NUMBER**

**DATE**