

NOTICE: THIS APPLICATION IS FOR CLAIMS-MADE AND REPORTED COVERAGE. READ THE ENTIRE APPLICATION CAREFULLY.

I. APPLICANT INFORMATION

Name of Applicant: _____
(Include names of all subsidiary or affiliated companies to be insured, or attach separate sheet, if necessary)

Principal Address: _____

City: _____ State: _____ Zip Code: _____

Mailing Address (if different): _____

City: _____ State: _____ Zip Code: _____

Telephone Number: _____ Fax Number: _____

Email: _____ Corporate Website Address: _____

II. COVERAGE REQUESTED

Requested Effective Date: _____

III. YOUR BUSINESS

1. Nature of business: _____

2. Description of operations: _____

3. Total annual revenues (indicate complete number, e.g., \$1,000,000): _____

4. Estimate total number of customer and/or employee records stored by you or by third parties on your behalf, either electronically or in physical files.

- 0-100,000
- 100,001-250,000
- 250,001-500,000
- Over 500,000
- I don't know

5. Does the Applicant use anti-virus software and a securely configured firewall to protect its network? Yes No

6. Does the Applicant utilize a cloud provider to store data? Yes No

If "Yes", please name the cloud provider: _____

If the Applicant utilizes more than one cloud provider to store data, please name the cloud provider storing the largest quantity of customer and/or employee records, including medical records, personal health information, social security numbers, bank account details, and credit card numbers.

For Question 7, if the answer is "No", PCI DSS Liability coverage will not be available.

7. Are you (or your credit card point of sale vendor, if applicable) PCI-DSS Compliant? Yes No

IV. LOSS HISTORY

If the answer to any of questions 8-10 is “YES”, please provide specific details on a separate page.

8. In the past 3 years, has the Applicant or any other person or organization proposed for this insurance:
- a) Received any complaints or demand letters, or been the subject of any litigation, government action or investigation, or other regulatory or legal proceedings involving matters of privacy injury, breach of private information, violation of privacy law, network security, identity theft, denial of service attacks, computer virus infections, theft or loss of confidential information, damage to third party networks, or the ability of third parties to rely on the Applicant’s network? Yes No
 - b) Sustained any unscheduled network outage or interruption for any reason? Yes No
 - c) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? Yes No
9. Does the Applicant or any other person or organization proposed for this insurance have knowledge of any security breach, privacy breach or other privacy-related event or incident, cyber extortion demand or threat, or allegations of breach of privacy? Yes No
10. Has any IT service provider that the Applicant relies on sustained an unscheduled network outage or interruption lasting longer than 4 hours within the past 3 years? Yes No
- If “Yes”, did the Applicant experience an interruption in business due to such outage or interruption? Yes No

V. ACKNOWLEDGEMENTS AND REPRESENTATIONS

1. **The undersigned represents that the statements, representations and information contained herein, or attached to this Application, are true and complete, and that reasonable efforts have been made to obtain sufficient information to facilitate the proper and accurate completion of this Application.**
2. **The undersigned acknowledges that the signing of this Application does not bind the undersigned to complete the insurance. The undersigned further acknowledges that the statements, representations, and information contained herein, or submitted with this Application (which shall be retained on file by the Underwriters and shall be deemed attached hereto, as if physically attached hereto), are material to the risk assumed by the insurer; that any policy will have been issued in reliance upon the truth thereof; and that this Application and all written statements and materials furnished to the Insurer in conjunction with this Application shall be deemed incorporated into and made a part of the policy, should a policy be issued.**
3. **Underwriters hereby are authorized to make any investigation and inquiry in connection with this Application as they may deem necessary.**
4. **The undersigned acknowledges and agrees that if the information supplied on this Application, or in any attachments, changes between the date of the Application and the effective date of the policy period, the Applicant will immediately notify the Underwriters of such change, and the Underwriters may withdraw or modify any outstanding quotations and/or agreement to bind the insurance.**
5. **For purposes of creating a binding contract of insurance by this Application, or in determining the rights and obligations under such a contract in any court of law, the parties acknowledge that a signature reproduced by either facsimile or photocopy shall have the same force and effect as an original signature, and that the original and any such copies shall be deemed one and the same document.**

Signed: _____ Print Name: _____

Must be signed by an authorized officer, partner or principal of the Applicant

Title: _____ Date (Mo/Day/Yr): _____

Applicant Organization: _____

Please Return to: greg.cooke@usi.com or fax to 610.537.2743

USI PrivaSafe 3.0 is cyber liability insurance that provides state-of-the-art coverage options to be custom-tailored for your clients' unique needs.

Our newest cyber coverage includes:

- Bodily Injury Liability (3rd Party) Sublimit - \$350,000
- Property Damage Liability (3rd Party) Sublimit - \$100,000
- Dependent System Failure Sublimit - \$1,000,000
- Bricking Coverage Sublimit - \$250,000
- Post Breach Event Remediation Sublimit - \$75,000
- Property Damage (1st Party) Sublimit - \$100,000
- TCPA Defense Sublimit, Court Attendance Sublimit, and Reward Expenses Sublimit
- Breach Event Costs outside the limit is included on most quotes
- Broad Cyber Crime Coverage available for loss of tangible property resulting from financial fraud
- Attorney Panel Endorsement available (Pre-approved counsel that can be utilized immediately)
- Option for a per-identity breach response limit instead of the typical dollar limit
- PCI DSS Liability now covered up to the policy limit on



NAS cyberNET®

Support & Risk Management

USI PrivaSafe 3.0 includes access to NAS CyberNET®—the online support center where your clients can connect with expert cyber risk advisors, training courses, sample policies and more. NAS CyberNET® helps your insureds mitigate the risk and impact of a cyber breach with services that include:

Cyber Security Training

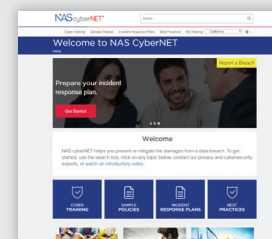
Data Security Basics
Social Engineering and Phishing
Ransomware Attacks

Compliance Material

State and Federal, Industry Specific
Data Protection Guidelines
Links to Government Sites

Cyber Security Best Practices

Data Privacy Guidelines
Risk Assessment & Fitness Checklist
Incident Response Planning



Expert Cyber Claims Handling from NAS

NAS' cyber claims team provides rapid response support for your clients. We handle over 2,000 cyber claims each year and with more than 20 in-house cyber claims team members, NAS provides expert service and support when clients need it most by:

- Quickly responding to initial claim notifications
- Assessing coverage and reviewing the claims process with the broker and policyholder
- Coordinating cyber expert service providers with policyholder to quickly address and resolve a cyber attack.



Proactive Cyber Services

Being insured isn't always the same as being prepared. We offer our cyber policyholders a range of discounted proactive services from leading cybersecurity experts. Services include:

- Network Security Assessments
- Table-top Incident Readiness Consulting
- Security Awareness Training
- Email Phishing Simulations
- PCI Compliance Reviews

Cyber Risk Scan (Coming Soon)

To help the insured better understand their risk and cyber vulnerabilities, beginning May 1, 2019 every PrivaSafe 3.0 quote will include a cyber risk summary with an overall rating of their public facing cyber security defenses.



Factors evaluated by the scan include Domain Security, Network Exposure, Web Application Risk, Web Traffic Encryption and Mail Server Security.

When the policy is issued, a comprehensive assessment will be provided. The full report will identify areas of cyber security risk and provide insight into different facets of an organization's readiness to defend against a cyber attack.

Industry Leading Expertise

Our team of incident response experts are leaders in the field and are here to help you. We have the experience and know-how to respond quickly and get your business back on track. The following is a partial list of experts with whom we are proud to collaborate:



NAS Insurance is a Lloyd's of London coverholder and benefits from Lloyd's of London's financial strength and robust capitalization.

Lloyd's reliability is reflected in its financial ratings:
AM Best: A (Excellent) Class XV
Standard & Poor's: A+ (Strong)

For more information, contact:

Peter Hedberg, Vice President, Northeast
 phedberg@nasinsurance.com | 646.693.7559

Jordan Rankell, AVP, West Coast
 jrankell@nasinsurance.com | 818.479.4305

Ari Giller, AVP, Midwest
 agiller@nasinsurance.com | 312.690.7111

Tina Porcelli Levine, AVP, Southeast
 tporcelli@nasinsurance.com | 818.479.4301

* Risk scan provided by ePlace Solutions, Inc.