

## APPLICATION for: **NetGuard® Plus**

Claims Made Basis. Underwritten by Underwriters at Lloyd's, London

Notice: The Policy for which this Application is made applies only to Claims made against any of the Insureds during the Policy Period. The Limit of Liability available to pay damages or settlements shall be reduced and may be completely exhausted by amounts incurred as defense costs. Defense costs shall be applied to the retentions.

Submission of this Application does not guarantee coverage.

**General instructions for completing this Application:** (Download application before entering data.)

- 1. Please read carefully and answer all questions. If a question is not applicable, so state by writing "Not Applicable".**
- 2. The completed Application should include all information relative to all subsidiaries and locations to be covered.**
- 3. The Application must be signed by an executive officer.**
- 4. Please read the Policy for which application is made (the "Policy") prior to completing this Application. The terms as used herein shall have meanings as defined in the Policy.**

### SECTION I. YOUR DETAILS

1. Name of Applicant: \_\_\_\_\_  
(Include names of all subsidiaries or affiliated companies to be insured; attach a separate sheet, if necessary)
- Applicant Type:     Individual     Corporation     Partnership     Other
- Headquarters Address: \_\_\_\_\_
- Mailing Address (if different): \_\_\_\_\_
- Telephone Number: \_\_\_\_\_ Fax Number: \_\_\_\_\_
- Email Address: \_\_\_\_\_
- Corporate Website Address: \_\_\_\_\_
- Nature of Business: \_\_\_\_\_

### SECTION II. YOUR BUSINESS

2. Date established: \_\_\_\_\_
3. Are any significant changes in nature or size (e.g., more than 20% increase in revenue) of Applicant's business anticipated over the next 12 months?     Yes     No
- If "Yes", please explain:** \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

**SECTION III. COVERAGE REQUESTED**

- 4. Proposed Effective Date: \_\_\_\_\_
- 5. Requested Retroactive Date: \_\_\_\_\_
- 6. Limit of Liability Desired:  
 \$500,000    \$1,000,000    \$2,000,000    \$3,000,000    \$4,000,000    \$5,000,000    Other \_\_\_\_\_
- 7. Retention Desired:  
 \$2,500    \$5,000    \$7,500    \$10,000    \$25,000    Other \_\_\_\_\_

**SECTION IV. EXPOSURE INFORMATION**

**ANNUAL REVENUE AND EXPOSURE BASE**

- 8. Total Annual Revenue:    \$\_\_\_\_\_
- 9. What percentage of the total annual revenue stated above is attributed to e-commerce? \_\_\_\_\_%
- 10. Please estimate total number of customer and employee records you store either electronically or in physical files.  
 Current number: \_\_\_\_\_    For the Next 12 Months: \_\_\_\_\_
- 11. Please estimate the total number of credit card transactions for the next 12 months: \_\_\_\_\_

**SECTION V. INFORMATION SECURITY CONTROLS**

- 12. Do you enforce a security policy that must be followed by all employees, contractors, or any other person(s) with access to your network?  Yes    No
- 13. Does your security and privacy policy include mandatory training for all employees?  Yes    No
- 14. Do all employees with financial or accounting responsibilities at your company complete social engineering training?  Yes    No
- 15. Are you HIPAA compliant?  Yes    No
- 16. Do you process, store, or handle credit card transactions?  Yes    No  
 If "Yes", are you PCI-DSS Compliant?  Yes    No
- 17. Do you collect zip codes from customers at point of sale?  Yes    No  
 If "Yes", are you compliant with the Song-Beverly Credit Card Act of 1971?  Yes    No
- 18. Do you use a cloud provider to store data?  Yes    No  
 If "Yes", please provide the name of the cloud provider: \_\_\_\_\_  
 If more than one provider is utilized, please list the provider that stores the most confidential information for the Applicant.
- 19. a) Do you require all third parties to whom you entrust sensitive or non-public personal information to contractually agree to protect such information using safeguards at least equivalent to your own?  Yes    No  
 b) Do you require that these third parties indemnify you in the event that they suffer a security/privacy breach?  Yes    No

**SECTION VI. FUNDS TRANSFER INSTRUCTION CONTROLS**

20. Does your wire transfer authorization process include:
- a) A wire request documentation form that includes getting proper authorization in writing?  Yes  No
  - b) A protocol that includes proper separation of authority?  Yes  No
  - c) A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer by direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment or funds transfer instruction/request was received?  Yes  No
  - d) A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information, and mailing addresses) by a direct call to that vendor, client, or customer using only the telephone number provided by the vendor, client, or customer before the change request was received?  Yes  No

**SECTION VII. COMPUTER & NETWORK SECURITY**

21. Does your virus or malicious code control program address the following: anti-virus on all systems, filtering of all content for malicious code, controls on shared drives and folders, CERT or similar vendor neutral threat notification services, removal of spyware and similar parasitic code?  Yes  No
22. Does your network have firewall protection that is securely configured?  Yes  No
23. Do you enforce a software update process that includes monitoring of vendors or automatically receiving notices from them for availability of security patches, upgrades, testing and installing critical security patches?  Yes  No  
 If "Yes", how frequently is this done?  Weekly  Within 30 days  More than 30 days
24. Do you test your security at least yearly to ensure effectiveness of your technical controls as well as your procedures for responding to security incidents (e.g., hacking, viruses, and denial of service attacks)?  Yes  No  
 If "Yes", does this include a network penetration test?  Yes  No
25. Do you allow any remote access to your network?  Yes  No  
 If "Yes", do you use two-factor authentication to secure remote access?  Yes  No
26. Do you retain non-public personal information and others' sensitive information only for as long as needed and when no longer needed irreversibly erase or destroy them using a technique that leaves no residual information?  Yes  No
27. Do you employ physical security controls to prevent unauthorized access to computer, networks and data?  Yes  No
28. Do you control and track all changes to your network to ensure that it remains secure?  Yes  No
29. Has there been a full, third party scan of your network carried out in the last year to check for intrusions and malware?  Yes  No
30. How long does it take to restore the Applicant's operations after a computer attack or other loss/corruption of data?  12 hrs or less  12-24 hrs  More than 24 hrs
31. Is all sensitive and confidential information that is transmitted within and from your organization encrypted using industry-grade mechanisms?  Yes  No
32. Is all sensitive and confidential information stored on your organization's databases, servers and data files encrypted?  Yes  No
33. If encryption is not in place for databases, servers and data files, are the following compensating controls in place:
- a) Segregation of servers that store confidential information?  Yes  No
  - b) Access control with role based assignments?  Yes  No

- 34. Does your organization store personal information on portable devices, including laptops, PDA's, back-up tapes, USB thumb drives and external hard drives?  Yes  No  
 If "Yes", is such data encrypted to industry standards?  Yes  No
- 35. How often is critical data backed up? \_\_\_\_\_
- 36. Within the past two years, have you passed an outside privacy audit or have you received a privacy certification?  Yes  No  
 If "Yes", have all recommendations been resolved?  Yes  No
- 37. Within the last two years, have you completed an internal audit or assessment to determine compliance with regulations or laws concerning the protection of privacy rights?  Yes  No  
 If "Yes", have all recommendations been resolved?  Yes  No
- 38. Have you developed any of the following written documents:
  - a) Incident Response Plan?  Yes  No
  - b) Business Continuity Plans (BCP) for identified critical cyber security events?  Yes  No
  - c) Disaster Recovery Plan (DRP) for identified critical cyber security events?  Yes  No
 If "Yes", are they tested annually?  Yes  No

**SECTION VIII. MEDIA**

- 39. Does the Applicant use material provided by others, such as content, music, graphics or video stream?  Yes  No  
 If "Yes", does the Applicant always obtain the necessary rights, licenses, releases & consents for the use of the materials provided by others?  Yes  No  
 Please describe below your process for obtaining necessary rights, licenses, releases & consents for the use of the materials provided by others.

---



---



---

- 40. Please describe the Applicant's procedures for removing potentially defamatory or infringing material. \_\_\_\_\_

---



---

**SECTION IX. LOSS HISTORY**

- 41. In the past 3 years, has the Applicant or any other person or organization proposed for this insurance:
  - a) Received any complaints or claims or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks, or the Applicant's customers' ability to rely on the Applicant's network?  Yes  No
  - b) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation?  Yes  No
  - c) Notified customers, clients, or any third party of any security breach or privacy breach?  Yes  No
  - d) Received any cyber extortion demand or threat?  Yes  No
  - e) Sustained any unscheduled network outage or interruption for any reason?  Yes  No
  - f) Sustained any property damage or business interruption losses as a result of a cyber-attack?  Yes  No
  - g) Sustained any losses due to wire transfer fraud, telecommunications fraud or a phishing attack?  Yes  No

- 42. Do you or any other person or organization proposed for this insurance have knowledge of any security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim?  Yes  No
- 43. Has any employee ever been disciplined for mishandling data or otherwise tampering with your computer network?  Yes  No
- 44. Has any service provider with access to the Applicant's network or computer system(s) 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 as a result of such outage or interruption?  Yes  No

*If the answer to any question in Section VII is "Yes", please provide full details of each claim, allegation, or incident on a separate page, including type and amount of costs, losses or damages incurred or paid (including amounts paid under insurance, if any) and any corrective measures and/or remediating steps taken to avoid such claim, allegation, or incident in the future.*

**SECTION X. WARRANTY AND REPRESENTATIONS**

1. The undersigned warrants and represents that the statements and information contained in 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. Signing of this Application does not bind the undersigned to complete the insurance; however, the Undersigned acknowledges and recognizes that the statements, representations, and information contained in or attached to this Application are material to the risk assumed by the Insurer; that any Policy will have been issued in reliance upon the truth thereof; that this Application shall be the basis of the contract should a Policy be issued; and that this Application, and all information 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. Underwriters hereby are authorized to make any investigation and inquiry in connection with this Application as they may deem necessary.
3. 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 inception date of the policy period, the Applicant will immediately notify the Insurer of such change, and, the Insurer may withdraw or modify any outstanding quotations and/or agreement to bind the insurance.
4. 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: \_\_\_\_\_  
(Authorized representative of applicant and/or policyholder)

Title: \_\_\_\_\_ Date (Mo/Day/Yr): \_\_\_\_\_

Applicant Organization: \_\_\_\_\_