

Network Security & Privacy Liability Application



AmTrust North America
An AmTrust Financial Company

*To be able to save this form after the fields are filled in, you will need to have Adobe Reader 9 or later. If you do not have version 9 or later, please download the free tool at: <http://get.adobe.com/reader/>.

Security National Insurance Company
(all states except: AZ, CT, DE, FL, LA and NJ)

Wesco Insurance Company
(applies to: AZ, CT, DE, FL and NJ)

AmTrust Insurance Company of Kansas
(LA only)

THE LIABILITY POLICY THAT MAY BE ISSUED BASED UPON THIS APPLICATION PROVIDES CLAIMS MADE COVERAGE WRITTEN ON A NO DUTY TO DEFEND BASIS. DEFENSE COSTS ARE INCLUDED WITHIN THE LIMIT OF LIABILITY AND REDUCE THE LIMIT OF LIABILITY AVAILABLE TO PAY SETTLEMENTS AND JUDGMENTS. PLEASE READ THE POLICY CAREFULLY.

Section 1 – General Information

Applicant (Parent Company): _____

Address: _____ City: _____ State: _____ Zip Code: _____

P.O. Box: _____ City: _____ State: _____ Zip Code: _____

Telephone: _____

Business Description: _____ SIC Code: _____

Year Operations Commenced: _____ Total assets at latest fiscal year end: \$ _____

Please list the Applicant's websites proposed for coverage:

- a. _____
- b. _____
- c. _____

Designated Chief Information Security Officer or individual or entity responsible for handling this role:

Name: _____ Title: _____ Email: _____

Contact information of individual responsible for breach response of the Applicant:

Name: _____ Title: _____ Email: _____

For purposes of this Application for coverage, "Applicant" means the Parent Company and any Subsidiary listed below, including any limited liability companies and joint ventures for which coverage is desired.

Section II – Current Coverage

Type of coverage:	Carrier	Limit	Indicate if Separate Limit	Retention	Premium	Expiration
Third Party Liability Coverages						
Network Security & Privacy Liability:	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____
Media Communications:	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____
Regulatory Defense & Penalties:	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____
First Party Coverages						
Computer Expert (Forensics):	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____
Privacy Notification:	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____
Public Relations:	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____
Cyber Extortion Threat:	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____
Business Interruption:	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____
PCI Fines and Expenses:	_____	\$ _____	<input type="checkbox"/>	\$ _____	\$ _____	_____

Section III – Network Security & Privacy Controls

1. Does the Applicant have a formal program in place to test or audit network security controls? Yes No
- a. How often are internal audits performed? _____
- b. How often are outside/third party audits performed? _____
- c. Have all vulnerabilities identified in a. and b. above been remedied? Yes No
2. Does the Applicant use firewall technology? Yes No
3. Does the Applicant use anti-virus software on all computer systems? Yes No
4. Are the Applicant's computer applications, software and operating systems kept current with the latest updates/patches? Yes No
5. Does the Applicant use intrusion detection software to detect unauthorized access to internal networks and computer systems? Yes No
6. Is user-specific, private, sensitive or confidential information stored on the Applicant's server(s) encrypted? Yes No
7. Are the Applicant's wireless transmissions protected using WPA/WPA2, IPSEC, or SSL? Yes No
8. Is all confidential information that is transmitted to/from, or stored within the Applicant's networks (including wireless networks) encrypted? Yes No
9. Are the Applicant's users able to store data to the hard drive of portable computers or portable media devices such as USB drives? Yes No
- a. If "Yes", does the Applicant encrypt data stored on laptop computers and portable media? Yes No
10. Are the Applicant's computer systems, applications and servers that collect confidential information segregated from the rest of the network? Yes No
11. Are the Applicant's computer systems, applications and servers backed up on a daily basis? Yes No
12. Is multi-factor authentication a requirement for accessing secure areas of the Applicant's network? Yes No
13. Are all system administrative accounts of the Applicant limited only to essential personnel? Yes No
14. Does the Applicant have a secondary computer system or site available if the primary resource becomes inoperative? Yes No
- a. How many hours before the secondary resource becomes operational? _____ hours
- b. What percentage of normal system operations can be handled via secondary sources? _____ %
15. Is remote network access restricted to VPN? Yes No
16. Is there a formal process in place to ensure that network privileges and physical access to the Applicant's facilities are revoked in a timely manner following an employee's separation from the Applicant? Yes No
17. Does the Applicant send or accept financial transactions intended for deposit via the use of remote deposit capture technology? Yes No
18. Does the Applicant use a third party provider for the following services?
- | | | | |
|--|---|---|---|
| <input type="checkbox"/> Managed Security Services | <input type="checkbox"/> Internet Service Provider | <input type="checkbox"/> Application Service Provider | <input type="checkbox"/> Website Hosting |
| <input type="checkbox"/> Disaster Recovery | <input type="checkbox"/> Data Destruction | <input type="checkbox"/> Credit Card Processing | <input type="checkbox"/> Data Archiving and Restoration |
| <input type="checkbox"/> Information Security Risk Assessments | <input type="checkbox"/> Vulnerability Assessment and Penetration Testing | | |
19. If applicable, do all vendor contracts:
- a. Indemnify/hold the Applicant harmless for vendor misconduct, errors, omissions or negligence? Yes No
- b. Outline the vendor's responsibility for safeguarding customer and confidential information and stipulate what security measures are provided by the vendor? Yes No
20. Does the Applicant maintain a formal, written:
- a. Information security & privacy policy? Yes No
- b. Data breach response plan? Yes No
- c. Security incident response plan? Yes No
- d. Disaster recovery/business continuity policy? Yes No
- e. Records retention and destruction policy? Yes No

Section IV – Regulatory Compliance

1. Is the Applicant currently compliant with the following regulations:
- a. Gramm-Leach-Bliley Act of 1999? Yes No
 - b. Identity Theft Red Flags under the Fair and Accurate Credit Transactions Act of 2003? Yes No
 - c. Payment Card Industry (PCI) Data Security Safeguard? Yes No

Section V – Media Communications

1. Has the Applicant screened all trademarks used by the Applicant for infringement with existing trademarks prior to first use? Yes No
2. Does the Applicant obtain written permission from website owners for the Applicant to “link” to or “frame” such individual or entity’s website? Yes No
3. Does the Applicant have a procedure in place to review content prior to posting? Yes No
- If “No”, please attach details on the Applicant’s procedures to avoid the posting of improper or infringing content.**
4. Does the Applicant have a procedure for responding to allegations that content created, displayed or published by the Applicant is libelous, infringing, or in violation of a third party’s privacy rights? Yes No

Section VI – Prior Knowledge and Claims History

1. Have there been during the last 5 years, or are there now pending, any claims or complaints, government actions, investigations or subpoenas with respects to allegations of failing to prevent unauthorized access to confidential information, failing to notify appropriate individuals of any such unauthorized access or failing to allow authorized users access to the Applicant’s computer systems? Yes No
- If “Yes”, please attach details for each claim.**
2. Has the undersigned or any proposed Applicant suffered any systems intrusions [i.e. unauthorized access or security breach] or denial of service attacks which impaired the functionality of its computer systems? Yes No
- If “Yes”, please attach details for each claim.**
3. Has the Applicant ever received any claims or complaints, or been subject to any government action, investigation or subpoena with respect to allegations that any content disseminated on or via the Applicant’s websites or company email, infringed on the intellectual property rights of another party or caused harm to the reputation of another party? Yes No
- If “Yes”, please attach details for each claim.**
4. Has the Applicant ever experienced an extortion attempt or demand with respect to its computer systems, or suffered a loss of money, securities or other property due to fraud committed by means of unauthorized or fraudulently entered computer instructions or code by someone other than an employee? Yes No
- If “Yes”, please attach details for each claim.**
5. Has the Applicant ever been subject to review by a team of PCI-DSS certified forensics security examiners as a result of an actual or suspected breach? Yes No
- If “Yes”, please attach details.**
6. Is the undersigned or any proposed Applicant aware of any fact, circumstance or situation involving any entity proposed for insurance, which he or she has reason to believe might result in a future claim? Yes No
- If “Yes”, please attach details for each claim.**

New Applicants:

It is understood and agreed that any claim arising from any prior or pending litigation or written or oral demand shall be excluded from coverage. It is further understood and agreed that if any fact, circumstance or situation which could reasonably be expected to give rise to a future claim exists, any claim or action subsequently arising therefrom shall also be excluded from coverage.

Renewal Applicants:

It is understood and agreed that if the undersigned or any insured has knowledge of any fact, circumstance or situation which could reasonably be expected to give rise to a future claim, then any increased limit of liability or coverage enhancement shall not apply to such fact, circumstance, or situation. In addition, any increased limit of liability or coverage enhancement shall not apply to any claim, fact, circumstance or situation for which the Insurer has already received notice.

Fraud Warning

Any person who knowingly and with intent to defraud any insurance company or another 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 may be a crime and may subject the person to criminal penalties.

ALABAMA, ARKANSAS, LOUISIANA, NEW MEXICO, RHODE ISLAND, VIRGINIA and WEST VIRGINIA: 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. In Alabama, Arkansas, Louisiana, Rhode Island and West Virginia that person may be subject to fines, imprisonment or both. In New Mexico, that person may be subject to civil fines and criminal penalties. In Virginia, penalties may include imprisonment, fines and denial of insurance benefits.

COLORADO: 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.

DISTRICT OF COLUMBIA: 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.

KENTUCKY and PENNSYLVANIA: Any person who knowingly and with intent to defraud any insurance company or other person files an Application for insurance or statement of claim containing 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. In Pennsylvania, and subjects such person to criminal and civil penalties.

FLORIDA: Any person who knowingly and with intent to injure, defraud or deceive the Insurer, files a statement of claim or an Application containing any false, incomplete or misleading information is guilty of a felony. In Florida it is a felony to the third degree.

KANSAS: An act committed by any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written, electronic, electronic impulse, facsimile, magnetic, oral, or telephonic communication or statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto.

MAINE: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or denial of insurance benefits.

MARYLAND: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or knowingly or willfully presents false information in an Application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

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

NEW YORK: Any person who knowingly and with intent to defraud any insurance company or any 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 shall also be subject to a civil penalty not to exceed five thousand dollars (\$5,000) and the stated value of the claim for each such violation.

OHIO: Any person who, with intent to defraud or knowing that he is facilitating a fraud against the Insurer, submits an Application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

OKLAHOMA: 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.

OREGON: 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 may be guilty of a crime and may be subject to fines and confinement in prison.

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

VERMONT: Any person who knowingly presents a false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law.

Representation Statement

The undersigned declares that, to the best of their knowledge and belief, the statements in this Application, any prior Applications, any additional material submitted, and any publicly available information published or filed by or with a recognized source, agency or institution regarding business information for the Applicant for the 3 years prior to the Policy's inception [hereinafter called "Application"] are true, accurate and complete, and that reasonable efforts have been made to obtain sufficient information from each and every individual or entity proposed for this insurance. It is further agreed by the Applicant that the statements in this Application are their representations, they are material and that the Policy is issued in reliance upon the truth of such representations.

The signing of this Application does not bind the undersigned to purchase the insurance and accepting this Application does not bind the Insurer to complete the insurance or to issue any particular Policy. If a Policy is issued, it is understood and agreed that the Insurer relied upon this Application in issuing each such Policy and any Endorsements thereto.

The undersigned further agrees that if the statements in this Application change before the effective date of any proposed Policy, which would render this Application inaccurate or incomplete, notice of such change will be reported in writing to the Insurer immediately.

Chief Executive Officer, President or Chairman of the Board:

Print Name: _____ Signature: _____

Title: _____ Date: _____

Agent Name: _____ License Number: _____

Agent Signature: _____

Please provide the following information with your submission:

- Copy of expiring Cyber Liability Declarations Page – New Applicants only.
- Latest report from any test or audit of network security controls performed internally or by a third party vendor.

Submit Application to:

banksubmissions@amtrustgroup.com

**AmTrust North America
Attention: Financial Institution Division**

800 Superior Avenue E., 21st Floor • Cleveland, OH, 44114

Phone: 866.327.6904 • Fax: 216.328.6251

Website: www.amtrustfi.com