



ACE Privacy Protection® Privacy & Network Liability Insurance Program Application

NOTICE

The Policy for which you are applying is written on a claims-made and reported basis. Only Claims first made against the Insured and reported to the Insurer during the Policy Period are covered subject to the Policy provisions.

The Limits of Liability stated in the Policy are reduced, and may be exhausted, by Claims Expenses. Claims Expenses are also applied against your Retention, if any. If you have any questions about coverage, please discuss them with your insurance agent.

INSTRUCTIONS

Completion of this application may require input from your organization's risk management, information technology, finance, and legal departments. Additional space may be needed to provide complete answers.

- Please type or print answers clearly.
- Answer **ALL** questions completely, leaving no blanks. If any questions, or part thereof, do not apply, print "N/A" in the space.
- Provide any supporting information on a separate sheet using your letterhead and reference the applicable question number.
- Check Yes or No answers
- This form must be dated and signed by the CEO, CFO, President, Risk Manager, or General Counsel of your company.

Underwriters will rely on all statements made in this application.

PLEASE ANSWER ALL QUESTIONS APPLICABLE TO COVERAGE FOR WHICH YOU ARE APPLYING.

All applicants must complete sections **I – IV** and **VII** of this application.

If coverage extension **D**, Electronic Media Liability, is required, please also complete section **V**, Internet Media Activities, which should be completed with the assistance of the applicant's legal department.

ADDITIONAL INFORMATION REQUIRED

Please submit the following documentation with the application:

1. Most recent annual report or 10K.
2. List of all material litigation threatened or pending (including plaintiff, cause of action and potential damages detail), which could potentially affect the coverage for which applicant is applying.
3. Loss runs for the last five years.
4. Copy of the privacy policy(ies) currently in use.
5. Executive summary of most recent network security assessment and/or PCI DSS audit, self-assessment, and/or scan.

I. INSURANCE INFORMATION

A. Coverage and Limits for which organization is applying

The ACE Privacy Protection® program consists of three standard coverage parts (A, B, C) and two coverage extension parts (E, F).

Please check the applicable blocks for types of coverage desired and indicate limits requested:

Coverage Part	Coverage Desired	Limit	Retroactive Date
<input type="checkbox"/> A. Privacy Liability	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$	___/___/___
<input type="checkbox"/> B. Identity Theft Response Fund	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$	
<input type="checkbox"/> B. Notification Expenses	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$	
<input type="checkbox"/> B. Crisis Management Expenses	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$	
<input type="checkbox"/> C. Network Security Liability	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$	___/___/___
<input type="checkbox"/> D. Internet Media Liability	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$	___/___/___
<input type="checkbox"/> E. Cyber Extortion	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$	___/___/___
<input type="checkbox"/> Regulatory Proceedings	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$	

B. Deductible and Coverage Dates Requested

Deductible Requested: \$50,000 \$100,000 \$250,000 Other: _____
 Proposed Effective Date: _____

C. Current Coverage and Loss Information

If the answer is yes to any of questions 2 – 10, please attach explanations. With respect to claims or litigation, include any pending or prior incident, event or litigation, providing full details of all relevant facts.

1. Does the company currently have General Liability, Privacy Liability, Network Liability, and/or other similar insurance in force? Yes No

If so, please complete the following for each policy:

Coverage Type:		Coverage Type:	
Name of Carrier:		Name of Carrier:	
Limits of Liability:		Limits of Liability:	
Deductible:		Deductible:	
Premium:		Premium:	
Expiry Date:		Expiry Date:	
Retroactive Date:		Retroactive Date:	

2. Has your company ever been declined for Privacy, Network Risk, or Media Liability insurance, or had an existing policy cancelled? Yes No

3. Has the company ever sustained a significant systems intrusion, tampering, virus or malicious code attack, loss of data, hacking incident, data theft or similar? Yes No

4. Is the company or any of its partners, directors or officers aware of, or are there any circumstances that may give, or have given, rise to a claim against the company or against this insurance policy? Yes No

5. In the last five years has your company experienced any claims or are you aware of any circumstances that could give rise to a claim that would be covered by this policy? Yes No
6. During the last three years, has anyone alleged that their personal information was compromised, or have you notified customers that their information was or may have been compromised, as a result of your activities? Yes No
7. During the last three years, have you received a complaint concerning the content of your website or other online services related to intellectual property infringement, content offenses, or advertising offenses? Yes No
8. During the last three years, have you been the subject of an investigation or action by any regulatory or administrative agency for violations arising out of your advertising or sales activities? Yes No
9. Has an employee ever been disciplined for mishandling data or otherwise tampering with your computer network? Yes No
10. Has the company sustained an unscheduled network outage over the past 24 months? Yes No

II. GENERAL INFORMATION

A. Applicant Information

Applicant Name: _____

Business Address: _____

Business Type: _____

Corporation Partnership LLC Other

Subsidiary Names
(if applicable): _____

Nature of Business: _____

Year Established: _____

Total Number of Employees: _____

URL Addresses for All Public-Facing Websites: _____

B. Risk Manager/Main Contact Information

Name: _____

Title: _____

Address: _____

Telephone: _____

Email Address: _____

C. Gross Revenues (including licensing fees)

	Domestic	Foreign	Total (dollars)	Percentage Online
Prior Year:	\$	\$	\$	%
Current Year (est.):	\$	\$	\$	%
Next Year (est.):	\$	\$	\$	%

III. RECORDS AND INFORMATION MANAGEMENT

1. Has your senior executive or Board of Directors established enterprise-wide responsibility for records and information management compliance with an individual manager? Yes No
 If so, is this a dedicated management position? Yes No
 If so, is this position currently filled by an experienced records/compliance officer? Yes No
2. Does a Board-approved, enterprise-wide policy covering records and information management compliance exist within your organization? Yes No
 If no, please describe: _____
 If yes, does it include enforceable provisions for non-compliance by employees, contractors, and third-party providers/partners? Yes No
3. Does your information asset classification program include a data classification standard (e.g., public, internal use only, confidential)? Yes No
 If so, does this standard also include mandated requirements for heightened protections (e.g., encryption, access control, data handling, retention and eventual destruction) that accompany each classification level? Yes No
4. Do you post a privacy policy on your Internet website? Yes No
 If so, has the policy been reviewed by a qualified attorney? Yes No
5. Does your organization have a current information asset inventory that is populated with all mission-critical sources of data and their named owners? Yes No
6. Have you identified all relevant regulatory and industry-supported compliance frameworks that are applicable to your organization? Yes No

	Compliant	Latest Audit
Gramm-Leach-Bliley Act of 1999:	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	_____
Health Insurance Portability and Accountability Act of 1996:	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	_____
Payment Card Industry (PCI) Data Security Standard:	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	_____
Other: _____	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____
7. Have you ensured that all sensitive business/consumer information that is transmitted within your organization or to/from other public networks has been encrypted using industry-grade mechanisms? Yes No

8. Have you ensured that all sensitive business/consumer information that resides within your organization's systems has been encrypted while "at-rest" within databases or other electronic data files? Yes No
9. Have you ensured that all sensitive business/consumer information that is physically transmitted – via tape or any other medium – between your organization's facilities and those of your business partners/service providers has been encrypted? Yes No
10. For computer equipment that leaves your physical facilities (e.g., mobile laptops, PDAs, BlackBerrys, and home-based desktops), have you implemented strong access control requirements and hard drive encryption to prevent unauthorized exposure of company data in the event these devices are stolen, lost or otherwise unaccounted for? Yes No
11. Does your organization follow established procedures for carrying out and confirming the destruction of data residing on systems or devices prior to their recycling, refurbishing, resale, or physical disposal? Yes No
12. Does your organization follow established procedures for carrying out and confirming the destruction of sensitive information in electronic and paper form prior to recycling or physical disposal? Yes No
13. Does your security awareness program include mandatory classes with measured testing (either through computer-based training or in-person participation) for all employees that may be expected to access, handle or process sensitive customer data as part of their assigned job responsibilities? Yes No
If no, please describe: _____
14. Does your organization follow established procedures for both "friendly" and "adverse" employee departures that include an inventoried recovery of all information assets, user accounts, and systems previously assigned to each individual during their full period of employment? Yes No
15. Does your organization employ a chief privacy officer who has enterprise-wide responsibility for meeting the obligations under the jurisdictional privacy and data protection laws that apply to the organization? Yes No
16. Has your organization – in response to California's SB 1386 and other similar laws - established a proactive procedure for determining the severity of a potential data security breaches and providing prompt notification to all individuals who may be adversely affected by such exposures? Yes No
17. Has your organization implemented procedures for honoring the specific marketing "opt-out" requests of your customers that are fully consistent with the terms of your currently published privacy policy? Yes No
 NA
18. Does your organization conduct regular reviews of your third-party service providers and partners to ensure that they adhere to your contractual and/or regulatory requirements for the protection of sensitive business/customer data that you entrust to their care for processing, handling, and marketing purposes? Yes No
 NA
- Do contracts with third-party service providers include indemnity provisions that protect you from any liability arising out of their loss of your sensitive information? Yes No

19. Have you configured your organization's Internet-facing Web sites and related systems so that no sensitive customer data resides directly on these systems? Yes No
- Have you configured your network to ensure that access to sensitive customer data is limited to properly authorized requests to internal databases/systems that are otherwise fully protected against Internet access? Yes No

IV. NETWORK OPERATIONS

A. Network Equipment

1. Approximate number of servers on your network: _____
2. Number of locations where servers are located: _____
3. Approximate number of external IP addresses on your network: _____
4. Average number of daily hits to your website: _____

B. Third Party Service Providers

Please identify third party vendor(s) providing any of the following services.

- Internet Service/Access: _____
- Website Hosting: _____
- Collocation Services: _____
- Managed Security Services: _____
- Broadband ASP Services: _____
- Outsourcing Services: _____
- Other (e.g. HR, POS): _____

C. Security Management

1. Do you have written policies in place which address:
 - Network security? Yes No
 - Appropriate use of network resources and the Internet? Yes No
 - Appropriate use of email? Yes No
2. Is there an organizational manager who is directly responsible for information security compliance operations? Yes No
3. Is there a program in place for employee awareness of the security policy? Yes No
4. Do you adhere to the policies of any of the following network security or information management standards?
 - ISO 17799: Yes No N/A
 - Sarbanes-Oxley Section 404: Yes No N/A
 - PCI Data Security Standard: Yes No N/A

If no to any of the above, please describe _____

D. Security Assessments

1. Has a network security assessment or audit been conducted within the past 12 months? Yes No

If yes, when was the last audit completed? _____ (Please attach copy of audit.)

2. Have you since complied with all recommendations from the audit? Yes No
3. Do you conduct periodic intrusion detection, penetration or vulnerability testing? Yes No

If yes, please detail what is done, the frequency, and who performs this work:

F. Firewall Management

1. Is firewall technology used at all Internet points-of-presence to prevent unauthorized access to internal networks? Yes No

If so, please describe brand name(s), model(s):

G. Antivirus Software

1. Does your company use antivirus software on all desktops, portable computers and mission critical servers? Yes No

If so please identify brand(s) or service providers:

2. Are antivirus applications updated in accordance with the software provider's requirements? If yes, how often? _____ Yes No

H. Software Maintenance

1. Is there an individual or internal organization responsible for the application of vendor-released patches and software fixes?? Yes No

If yes, please identify (name/title):

2. Are patches implemented on network appliances (routers, bridges, firewalls, etc.) to mitigate current vulnerabilities? Yes No

If yes, how often are patches installed? _____

I. Data and Systems Backups

1. Are your systems backed up on a daily (or more regular) basis? Yes No

If not, how often are systems backed up? _____

2. Are data backups stored offsite? Yes No

3. Are data recover and restoration procedures tested? Yes No

If yes, how frequently? _____

J. System and Security Logs

- 1. Do you actively maintain system logs on all mission-critical servers and appliances? Yes No
 - 2. Do you actively maintain security logs on all mission-critical servers and appliances? Yes No
 - 3. Are logs regularly checked for irregularities, intrusions or violations? Yes No
If yes, how often are logs checked, and who hold this responsibility?
-

K. Password Maintenance

- 1. Are documented procedures in place for user and password management? Yes No
If yes, are they monitored for compliance? Yes No
- 2. Are users required to use non-trivial passwords of at least six characters? Yes No

L. Physical Security

- 1. Are your dedicated computer rooms physically protected? Yes No
If yes, describe the protection (e.g. burglar alarms, etc.).
 - 2. How is access controlled or limited (e.g. key cards, biometrics, etc.)?
-

M. Disaster Recovery / Business Continuity Planning

- 1. Are system backup and recovery procedures documented and tested for all mission-critical systems? Yes No
 - 2. Do you have a written disaster recovery and business continuity plan for your network? Yes No
 - 3. Is the plan tested? If yes, describe frequency and extent of testing: Yes No
-

N. Personnel Management

- 1. Are background checks performed on applicants for positions of authority over the network? Describe: _____ Yes No
- 2. Are formal processes in place to ensure that network privileges are revoked in a timely manner following an employee's termination or resignation? Yes No

O. Payment Card Industry Data Security Standard (PCI DSS)

- 1. Are you subject to the PCI DSS? Yes No
If yes, what level requirement? 1 2 3 4
 - 2. Have you achieved PCI Compliance? If no, please describe current status: Yes No
 - 3. What percentage of your most recent PCI audit was identified as adequate or 'in place'?
 - 4. For those standards that were identified as either inadequate or 'not in place', how many have been implemented since the last audit? Please describe:
-

V. INTERNET MEDIA ACTIVITIES

Please complete this section if you are applying for coverage part D, Internet Media Liability Extension.

A. Internet Activities

Activities performed over your company's Internet sites:
Please check all that apply.

- electronic publishing, marketing, dissemination, or distribution of original works
- advertising the products or services of other companies for a fee
- buying or selling of goods, products or services
- collection or transmission of sensitive financial information
- legal or financial advice
- medical or health advice
- other personal advice services such as counseling
- website services or products to international customers/subscribers
- auction, exchange, or hub services
- files for download
- bulletin board(s) or chat room(s) on your website
- gambling or adult entertainment services
- operation of intranets
- operation of extranets or virtual private networks

B. Procedures for Information Management

1. Does your company use material provided by others, such as content, music, graphics or video stream, on your web site? Yes No
 - a. If yes, do you always obtain written licenses and consent agreements for the use of these materials? Yes No
 - b. If yes, please describe the process for obtaining written licenses and consent agreements for the use of these materials:

2. Please describe established procedures in place for the formal review of content/material for your web sites or Internet services:

3. Does your company have an established procedure for editing or removing from your website libelous or slanderous content, or content that infringes the intellectual property rights of others (copyrights, trademarks, trade names, etc.)? Yes No

4. Does your website, system or network request and capture third party information? Yes No

If yes, please check all that apply:

- customer/subscriber names and addresses
- credit or debit card numbers
- social security numbers
- credit history and ratings
- medical records or personal health information
- intellectual property of others

bank records, investment data or financial transactions

other (please describe): _____

5. Has legal counsel checked that your domain name(s) and metatags do not infringe on another's trademark? Yes No
6. Does your company have a written and posted privacy policy on your site(s)? *If yes, when was this last updated?* _____ Yes No
7. Does your company have a non-disclosure policy? Yes No
8. Is sensitive, personal or confidential information located behind a firewall?
If yes, are strict access controls in place? Yes No
9. Is sensitive, personal or confidential information encrypted? Yes No
If no, please describe: _____
10. Does your organization sell or share individual subscriber or user identifiable information with other internal or external entities? Yes No
If yes, please describe: _____

C. Bulletin Board / Chat Room Administration

If you offer a bulletin board or chat room on your web site, please answer the following:

1. Who manages the bulletin board/chat room (in-house, subcontracted, etc.)?
2. If subcontracted, do you require, 'hold harmless' agreements for liabilities arising out of bulletin boards and/or chat rooms? Yes No
3. Can you remove any postings at your sole discretion? Yes No
4. Does the agreement with your ISP allow you to do so? Yes No

VI. FRAUD NOTICES

NOTICE TO ARKANSAS, LOUISIANA, RHODE ISLAND AND WEST VIRGINIA 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 of the third degree.

NOTICE TO KENTUCKY APPLICANTS: Any person who knowingly and with 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 knowingly 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 MARYLAND APPLICANTS: Any person who knowingly and willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly and willfully 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 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 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 CIVIL FINES AND CRIMINAL 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 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 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 OREGON APPLICANTS: 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 information for the purpose of misleading, commits a fraudulent insurance act, which may be a crime and may subject such person to criminal and civil penalties.

NOTICE TO PENNSYLVANIA APPLICANTS: 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 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 TENNESSEE, VIRGINIA AND 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.

NOTICE TO ALL OTHER APPLICANTS:

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 INFORMATION FOR THE PURPOSE OF MISLEADING, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME AND MAY SUBJECT SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

VII. DECLARATION AND CERTIFICATION

ALL APPLICANTS MUST COMPLETE THIS SECTION.

BY SIGNING THIS APPLICATION, THE APPLICANT WARRANTS TO THE INSURER THAT ALL STATEMENTS MADE IN THIS APPLICATION INCLUDING ATTACHMENTS, ABOUT THE APPLICANT AND ITS OPERATIONS ARE TRUE AND COMPLETE, AND THAT NO MATERIAL FACTS HAVE BEEN MISSTATED IN THIS APPLICATION OR CONCEALED. COMPLETION OF THIS FORM DOES NOT BIND COVERAGE. THE APPLICANT'S ACCEPTANCE OF THE INSURER'S QUOTATION IS REQUIRED BEFORE THE APPLICANT MAY BE BOUND AND A POLICY ISSUED.

THE APPLICANT AGREES TO COOPERATE WITH THE INSURER IN IMPLEMENTING AN ONGOING PROGRAM OF LOSS-CONTROL AND WILL ALLOW THE INSURER TO REVIEW AND MONITOR SUCH PROGRAMS THAT THE APPLICANT UNDERTAKES IN MANAGING ITS TECHNOLOGY EXPOSURES.

Signature of the Applicant's CEO, CFO,
President, Risk Manager, or General Counsel:

Signature of the Applicant's Broker/Agent:

Print Name

Print Name

Title

Date

Date

Signed by Licensed Resident Agent

(Where Required By Law)

FOR FLORIDA APPLICANTS ONLY:

Agent Name: _____

Agent License Identification Number: _____

FOR ARKANSAS, MISSOURI AND WYOMING APPLICANTS ONLY:

PLEASE ACKNOWLEDGE AND SIGN THE FOLLOWING DISCLOSURE TO YOUR APPLICATION FOR INSURANCE:

THE APPLICANT UNDERSTANDS AND ACKNOWLEDGES THAT THE POLICY FOR WHICH IT IS APPLYING CONTAINS A DEFENSE WITHIN LIMITS PROVISION WHICH MEANS THAT CLAIMS EXPENSES WILL REDUCE THE POLICY'S LIMITS OF LIABILITY AND MAY EXHAUST THEM COMPLETELY. SHOULD THAT OCCUR, THE APPLICANT SHALL BE LIABLE FOR ANY FURTHER CLAIMS EXPENSES AND DAMAGES.

Applicant's Signature:

(Must be signed by a CEO, CFO, President,
Risk Manager, or General Counsel of the Applicant)

Print Name and Title

_____/_____/_____
Date (Mo./Day/Yr.)