



Network Risk Insurance Application

App No _____ of _____

Date of Application _____ Name of Dealership _____
 Proposed Effective Date _____ DBA _____
 Business is _____
 Dealer Group _____ Year Established _____
 Street Address _____ City _____ County _____
 Post Office Box _____ City _____ State _____ Zip Code _____

GENERAL INFORMATION

Majority Owner's Name _____ Phone # _____ Majority Owners DOB _____
 Tax ID No. _____ Majority Owner Active Yes No
 Years of Experience Managing Dealerships _____

List all Owners of Dealership ***Use Separate Sheet if Necessary**

Name	% Ownership	Active Y/N
		<input type="checkbox"/> Yes <input type="checkbox"/> No
		<input type="checkbox"/> Yes <input type="checkbox"/> No
		<input type="checkbox"/> Yes <input type="checkbox"/> No

List all other Dealerships under same Majority Ownership for which application is not attached.

Dealership Name	% Ownership	City	State

* If application is not attached please explain: _____

Are there any Foreign Operations: Yes No If Yes, explain: _____

List and describe all other Subsidiary Operations and Companies ***Use Separate Sheet if Necessary**

Details _____

Dealership Contact Information

General Manager _____
 Phone # _____ Fax _____ E-Mail _____
 Accounting Contact _____
 Phone # _____ Fax _____ E-Mail _____
 Name of Person to receive Correspondence from the Company _____
 Mailing Address _____ City _____ State _____ Zip _____
 Phone # _____ Fax _____ E-Mail _____

PRODUCER INFORMATION

Producer Code _____ Producer _____
 Agency Name _____ Phone # _____ Fax _____
 Street Address _____ City _____ County _____
 Email _____ State _____ Zip code _____
 Post Office Box _____ City _____ State _____ Zip code _____

Operations

1. Number of Employees: _____
2. URL Addresses for All Public-Facing Websites: _____
3. Gross Revenues:

	Domestic	Foreign	Total
Prior Year:			
Current Year (est.):			
Next Year (est.):			

4. Products and Services Offered:
Please describe: _____

Coverage Selection

A. Limit, Deductible and Coverage Dates Requested

Note: The program is available in two formats.

Option 1: The standard format is available to all companies regardless of revenues and provides full limits for each coverage part required.

Option 2: The small business format is available to companies with current year revenues below \$25 million, and provides full limits for Coverage A, Digital Asset Loss, with sub-limits applied to the other coverages as detailed below.

Option 1: Standard Program *(all revenue classes eligible):*

1. Coverages Required

- A. Digital Asset Loss
- B. Cyber Extortion Threat
- C. Security Failure Notification Loss
- D. Business Interruption
- E. Contingent Business Interruption *(please check if required)*
We will assume all coverages are requested, with the exception of E. Contingent Business Interruption. We will assume Contingent Business Interruption coverage is required only if **Qualified Service Providers** are named below.

2. Requested Limits and Deductible:

Limits Requested:	<input type="checkbox"/> \$1,000,000	<input type="checkbox"/> \$3,000,000	<input type="checkbox"/> \$5,000,000	<input type="checkbox"/> Other:
Deductible Requested:	<input type="checkbox"/> \$25,000	<input type="checkbox"/> \$50,000	<input type="checkbox"/> \$100,000	<input type="checkbox"/> Other:

3. Business Interruption/ Contingent Business Interruption Waiting Period:

- 8 hours (minimum)
 12 hours
 24 hours
 Other

4. Proposed Effective Date: _____

5. Will you require coverage for the failure of key network service providers? Yes No

If you answered Yes, please identify all third party vendors and service providers to be considered **Qualified Service Providers**.

Key Service Provider	Services Provided	Approx. Contract Value	Contract Duration

Option 2: Small Business Program (companies with revenues under \$25 million eligible)

Package 1

Coverage	Limit	Deductible
Coverage A: Digital Asset Loss	\$ 1,000,000	\$ 10,000
Coverage B: Cyber Extortion Threat	\$ 100,000	\$ 10,000
Coverage C: Security Failure Notification Loss	\$ 50,000	\$ 10,000
Coverage D: Business Interruption Loss	\$ 2,500/hour, with \$ 250,000 sub-limit	8 hours

Package 2

Coverage	Limit	Deductible
Coverage A: Digital Asset Loss	\$ 3,000,000	\$ 25,000
Coverage B: Cyber Extortion Threat	\$ 250,000	\$ 25,000
Coverage C: Security Failure Notification Loss	\$ 100,000	\$ 25,000
Coverage D: Business Interruption Loss	\$ 5,000/hour, with \$ 500,000 sub-limit	8 hours

Package 3

Coverage	Limit	Deductible
Coverage A: Digital Asset Loss	\$ 5,000,000	\$ 50,000
Coverage B: Cyber Extortion Threat	\$ 250,000	\$ 25,000
Coverage C: Security Failure Notification Loss	\$ 100,000	\$ 25,000
Coverage D: Business Interruption Loss	\$ 7,500/hour, with \$ 1,000,000 sub-limit	8 hours

3. Proposed Effective Date: _____

B. Current Coverage and Loss Information:

1. Does the company currently have network risk or other similar insurance in force? Yes No

If yes, please complete the following:

Coverage Type	Name of Carrier	Limit	Deductible	Premium	Expiry Date

If the answer is yes to any of questions 2-5, please attach explanations. With respect to claims or litigation, include any pending or prior incident(s), event(s) or litigation, providing full details of all relevant facts.

2. Has your company ever been declined for network risk 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. Has an employee ever been disciplined for mishandling data or otherwise tampering with your computer network? Yes No

5. Has the company sustained an unscheduled network outage over the past 24 months? Yes No

Comments: _____

Information Management

A. Internet Activities:

Activities performed over your company's Internet sites:

Please check all that apply.

- Buying or selling of goods, products or services
- Collection or transmission of sensitive financial information
- Operation of intranets
- Operation of extranets or virtual private networks
- Auction, exchange, or portal services
- Files for download
- Gambling or adult entertainment services

Comments: _____

B. Procedures for Information Management

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

Is sensitive, personal or confidential information located behind a firewall?

Yes No

If yes, are strict access controls in place?

Yes No

Is encryption technology used when transmitting sensitive information?

Yes No

Comment: _____

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 average daily hits to your website:

Comment: _____

B. 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?
- British Standard 7799 Yes No
- ISO 17799 Yes No
- Sarbanes-Oxley Sec. 404 Yes No

Comment: _____

C. Security Assessments

1. Has a network security assessment or audit been conducted within the past 12 months? Yes No
- If yes when was the assessment completed?
- Please attach a copy of the assessment executive summary.
2. Were all recommendations from the audit complied with? Yes No
- If no, please identify areas where recommendations have not been complied with, with reason(s) for noncompliance
3. Do you conduct periodic intrusion detection, penetration or vulnerability testing? Yes No
- If yes, please detail what is done and who performs this work:

Comment: _____

D. 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):

Comment: _____

E. 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? Yes No
- If yes, how often?

Comment: _____

F. 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?

Comment: _____

G. 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?

Comment: _____

H. 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?

Comment: _____

I. 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

Comment: _____

J. 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? Yes No

If yes, describe frequency of testing:

Comment: _____

K. Personnel Management

- 1. Are background checks performed on applicants for positions of authority over the network? 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

NOTICE TO THE APPLICANT

A. The applicant represents to the best of its knowledge and belief that the statements set forth herein are true and complete.

B. The applicant agrees that after receipt of the completed application form, underwriters have five working days to either confirm or deny coverage. It is also agreed this application shall be the basis of insurance and will be attached to and made part of the policy should a policy be issued.

C. The applicant further represents that if the information supplied on this application changes between the date of the application and the inception date of the policy period, the applicant will immediately notify the underwriter of such a change, and the underwriter may modify or deny coverage.

Signed: _____ Date: _____
Authorized signature of a Principal or Officer

Print Name: _____ Title: _____

(Must be signed and dated no more than 45 days prior to binding)

GENERAL FRAUD STATEMENT

ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR ANOTHER 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 AND SUBJECT THE PERSON TO CRIMINAL AND [NY: SUBSTANTIAL] CIVIL PENALTIES. IN THE DISTRICT OF COLUMBIA, LOUISIANA, MAINE, TENNESSEE AND VIRGINIA, INSURANCE BENEFITS MAY ALSO BE DENIED.

OWNER/AUTHORIZED OFFICER SIGNATURE OF APPLICANT

I HEREBY AUTHORIZE AUTOMOTIVE RISK MANAGEMENT & INSURANCE SERVICES, INC. TO OBTAIN A LOSS HISTORY FROM MY CURRENT AND PRIOR INSURANCE CARRIER(S) AND TO SECURE CREDIT, MOTOR VEHICLE, AND LOSS CONTROL REPORTS AS NEEDED.

THE PRODUCER INDICATED ON PAGE ONE IS THE AGENT OF RECORD FOR INSURANCE MATTERS AS THEY PERTAIN TO AUTOMOTIVE RISK MANAGEMENT & INSURANCE SERVICES, INC'S DEALERSHIP INSURANCE PROGRAMS.

THE INFORMATION CONTAINED IN THIS APPLICATION (S) IS TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE. SIGNING THE APPLICATION (S) DOES NOT BIND THE UNDERWRITER TO OFFER NOR THE APPLICANT TO ACCEPT INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION SHALL BE THE BASIS OF THE INSURANCE WILL BE ATTACHED AND MADE PART OF THE POLICY SHOULD THE POLICY BE ISSUED.

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, PHOTOCOPY OR EMAIL SHALL BE THE SAME FORCE AND EFFECT AS AN ORIGINAL SIGNATURE AS AN ORIGINAL SIGNATURE AND THAT THE ORIGINAL AND ANY SUCH COPIES SHALL BE DEEMED ONE AND THE SAME DOCUMENT.

Signature of Owner or Authorized Officer Date

Print Name Title

PRODUCER RECOMMENDATION

I PERSONALLY RECOMMEND THIS DEALERSHIP FOR COVERGE. THIS DEALERSHIP IS HANDLED BY ME PERSONALLY AND NO OTHER PRODUCER IS INVOLVED UNLESS INDICATED AS A SUB-PRODUCER.

Producer and Authorized Representative Date