SUPPLEMENTAL APPLICATION FOR NETWORK SECURITY ENDORSEMENT

NOTICE: THE POLICY FOR WHICH APPLICATION IS MADE, SUBJECT TO ITS TERMS, APPLIES ONLY TO ANY CLAIM MADE DURING THE POLICY PERIOD. AMOUNTS INCURRED AS COSTS, CHARGES AND EXPENSES SHALL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO THE RETENTIONS.

Please fully answer all questions and submit all requested information and supplemental forms. Terms appearing in bold face in this Application are defined in the Policy and have the same meaning in this Application as in the Policy. If you do not have a copy of the Policy, please request it from your agent or broker. This Application, including all materials submitted herewith, shall be held in confidence.

1. How many of the following comprise the Applicant's network:
   - Server computers? _____
   - Workstation computers? _____
   - Authorized user accounts? _____
   - Geographically distinct LAN sites? _____

2. ON-LINE SERVICE CONTROLS
   Do you have a qualified attorney review all content prior to posting? ☐Yes ☐ No

   If yes, does the review include screening the content for the following?
   - Copyright Infringement ☐Yes ☐No
   - Trademark Infringement ☐Yes ☐No
   - Invasion of Privacy ☐Yes ☐No

   Do you have a policy for removing controversial material: (libelous, slanderous, etc) from your On-line Service? ☐Yes ☐No ☐N/A

3. Do you have a policy for removing infringing material (copyright, trademark, etc) from your On-line Service? ☐Yes ☐No ☐N/A

4. Have you ever received a complaint concerning the content of your On-line Service (libelous, slanderous, copyright, trademark, etc)? ☐Yes ☐No ☐N/A

   If Yes, how did you respond to such complaints and in what time frame?

   _____

5. COMPUTER SYSTEMS CONTROLS
   Has the Applicant suffered any known intrusions (i.e., unauthorized access) of its Computer Systems in the most recent past twelve (12) months? ☐Yes ☐No ☐N/A

   If Yes,
   How many intrusions occurred? ____
   If any damage was caused by any such intrusions, including lost time, lost business income, or costs to repair any damage to systems or to reconstruct data or software, describe the damage that occurred, and state value of any lost time, income and the costs of any repair or reconstruction:

Describe the response taken by the Applicant to the intrusions. _____

_____

_____

6. Please indicate which of the following information systems Policies and Procedures the Applicant has published and distributed to employees:

_____ Information system access regulations and controls,
_____ "Acceptable Use" standards,
_____ The company's right to monitor employee computer use and activity, including reading e-mails and monitoring website activities,
_____ Acceptable e-mail use,
_____ Acceptable internet use,
_____ Password discipline,
_____ Remote access,
_____ Incident response, handling, and reporting,
_____ Standards of communication for proprietary, sensitive, and confidential materials, and
_____ Responses to threatening, malicious, or unprofessional communications.

7. Does the Applicant require positive acknowledgement from each employee of their understanding and agreement with the above policies and procedures? ☐Yes ☐No

8. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its Computer Systems? ☐Yes ☐No

If yes, indicate how frequent such training is provided: _____

9. Does the Applicant have a disaster recovery program? ☐Yes ☐No
If Yes, please attach:

10. Are the Applicant's internal networks and/or Computer Systems subject to third party audit or monitoring (including ethical hacking for security purposes)? ☐Yes ☐No

If Yes, please summarize the scope of the service provided: _____

11. Has the Applicant undergone any business merger or acquisition that resulted in the merger of information systems in the most recent past three (3) years? ☐Yes ☐No

If yes, describe: _____

12. COMPUTER SYSTEM ACCESS PROTECTON

A. Does the Applicant provide remote access to its Computer Systems? ☐Yes ☐No
If Yes,
How many users have remote access? _____
Is remote access restricted to Virtual Private Networks (VPNs)? ☐Yes ☐No

If the answer is No, describe the extent to which other remote access is allowed, such as modem dial-in accounts, Remote Access Servers (RAS), or dedicated Frame Relay (FR) communications. _____

_____

B. Please indicate which of the following password disciplines the Applicant enforces via automated system or software settings:
_____ Passwords must contain at least eight (8) characters. If not, what is the minimum number of characters? _____
_____ Passwords must contain a mix of letters and one or more numbers and/or special characters (*()&%$#).
____ Passwords must be changed at least every 30 days. If not, how often? _____
_____ Old passwords may not be re-used.
_____ Passwords may not be a word found in a standard dictionary of the English language.

C. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? ☐Yes ☐No

D. Does the Applicant regularly compare all associated computer access and user accounts with some comprehensive employee record, such as payroll lists, to identify unauthorized or "extra" user accounts? ☐Yes ☐No

If the answer to either of questions 12.C.or 12. D. is no, describe any procedures used to assure that user accounts are valid: _____

_____

E. Does the Applicant use commercially available firewall protection systems to prevent unauthorized access to internal networks and computer systems? ☐Yes ☐No

F. Does the Applicant use intrusion detection software to detect unauthorized access to internal networks and Computer Systems? ☐Yes ☐No

G. Does the Applicant accept payment on-line for goods sold or services rendered? ☐Yes ☐No
If Yes, do you use commercially available software to ensure that these systems are secure? ☐Yes ☐No

H. Does the Applicant employ Anti-Virus software? ☐Yes ☐No
If Yes, is it company policy to up-grade the software as new releases/improvements become available? ☐Yes ☐No
If the answer is no, how often do you upgrade your Anti-Virus software with new releases?

_____

13. DATA ENCRYPTION PROCEDURES

A. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted? ☐Yes ☐No
If Yes, describe the types of 1) internal and 2) external communications which are encrypted.

_____