INTELLECT
Cyber Endorsement Supplemental Application

1. Please detail which of the following data types you store on your network or on your hosting provider's site *(check all that apply)*:

- ☐ Social Insurance Numbers
- ☐ Social Security Numbers
- ☐ Driver's License Numbers
- ☐ Geo-location Data
- ☐ Payment Card Details
- ☐ Medical records/Health information
- ☐ E-mail Addresses
- ☐ Trade secrets/ Intellectual property of others
- ☐ Individual names and addresses
- ☐ Bank Accounts and/or Routing number
- ☐ Bank records/details (Customers and/or employees)
- ☐ Credit History and rating
- ☐ Other: please describe: _____

2. Approximately how many private individuals do you hold sensitive data on?

☐ 0 ☐ 1 to 1,000 ☐ 1,001 to 5,000 ☐ 5,001 to 10,000 ☐ 10,001 to 25,000 ☐ 25,001 to 50,000 ☐ > 50,000

3. What percentage of these individuals reside in the United States?

☐ 0% ☐ <25% ☐ 26% to 50% ☐ 51% to 75% ☐ >75%

4. Is any of the information regulated by privacy, consumer protection, and/or data protection regulations in Canada (such as but not limited to PIPEDA, Privacy Act, PHIPA [Ontario], etc.) or the United States (such as but not limited to HIPPA/HITECH, GLB, FCRA/ FACTA, 201 CMR 17.00 [Massachusetts], etc.) or other laws or legislation protection and personal information? ☐ Yes ☐ No

5. Is personally identifiable data shared, sold or released to third parties? ☐ Yes ☐ No

6. Are there specific privacy data security provisions in your sub-contracting agreement? ☐ Yes ☐ No

7. Is there a document, data, and equipment retention and destruction policy? ☐ Yes ☐ No

8. Is training provided for employees on privacy, data security and related issues? ☐ Yes ☐ No

9. In all cases do hiring procedures include the following? *(Check all that apply)*

☐ Education background checks ☐ Criminal checks ☐ Work history

10. Is all sensitive data encrypted while standing and during transmission? ☐ Yes ☐ No

If yes, please name the encryption technologies used: _____

11. Is there a virus protection program in place? ☐ Yes ☐ No

12. Are there firewalls in place? ☐ Yes ☐ No

If yes, do firewalls have an Intrusion Detection system? ☐ Yes ☐ No

13. Are there security threats and incidents logged and investigated? ☐ Yes ☐ No

14. Does your company perform routine software updates and patch installations? ☐ Yes ☐ No

15. Are documented procedures in place for users and password management? ☐ Yes ☐ No

If yes, are they monitored for compliance? ☐ Yes ☐ No

16. Are users required to use non-trivial password of at least six characters? ☐ Yes ☐ No

17. Are all associated computer access and user accounts terminated when an employee leaves? ☐ Yes ☐ No

18. Does your company provide mobile devices or laptops for their employees? ☐ Yes ☐ No

a) Approximately how many devices are in circulation?_____

b) Is sensitive or confidential information stored on these devices? ☐ Yes ☐ No

c) Is there a security and usage policy in place? ☐ Yes ☐ No

d) Are laptop users required to authenticate through a secure VPN? ☐ Yes ☐ No

e) Is the same level of protection used as desktops within the office? ☐ Yes ☐ No

f) Are employees allowed to use their personal devices (including computers) for work usage? ☐ Yes ☐ No

g) Do all smartphones using/accessing company system resources have anti-virus software installed and regularly updated? ☐ Yes ☐ No

h) Do you utilize enterprise device management solutions to administer patch management, software updates, antivirus and/or other company wise updates to smartphones? ☐ Yes ☐ No

i) Are remote wipe capabilities enabled on all company used smart phones, laptops, and tablets in case the device is lost or stolen? ☐ Yes ☐ No

19. Is there an employee web usage policy in place? ☐ Yes ☐ No

If yes, is access restricted to inappropriate website or social media? ☐ Yes ☐ No

20. Are you aware of any circumstances that could result in a data breach/privacy claim or suit? ☐ Yes ☐ No

If yes, please provide details: _____

_____

21. During the past five years, has the Applicant's business experienced any type of network breach or release of privacy data? ☐ Yes ☐ No

If yes, please provide details including subsequent remedial measures put in please since the incident to avoid similar situations in the future:_____

_____

APPLICANT ACKNOWLEDGMENT

For the purposes of this application, the authorized representative of all person(s) and entity(ties) proposed for this insurance declare that, to the best of his/her knowledge and belief, after reasonable inquiry, the statements in this application, and in any attachments, are true and complete.

Signature of Authorized Representative: _____ Date: _____

PLEASE PRINT CLEARLY

Name of Authorized Representative: _____ Title: _____

MUST BE SIGNED BY A PRINCIPAL OR PARTNER