ASCENT™
UNDERWRITING

Privacy Questionnaire

You may provide any further additional information by means of a separate attachment if necessary.

1 General Information

a. Name(s) of Applicant

2 Operational Information

a. How many PII's are retained within your computer network, databases and records?
(PII is defined as a personally identifiable record on an individual that can be used to identify, contact or locate a single individual)

b. Identify the type of PII retained on your network

1. Payment card data Yes ☐ No ☐ 2. Healthcare data Yes ☐ No ☐ 3. Other PII Yes ☐ No ☐

If you have answered 'Yes' to b3. please provide details of the nature of this PII.

3 Business Continuity

a. Briefly describe your recovery/continuity plans to mitigate or avoid business interruption due to network failure, which may include outsourcing, additional employment, system redundancy etc.

b. Is this plan regularly tested and updated? Yes ☐ No ☐

c. Have you recently carried out a network security audit? Yes ☐ No ☐

If 'Yes', who performed the audit and when was it completed?

Audited by | DD | MM | YY

d. Was any serious concern raised with any aspect of the network? Yes ☐ No ☐

If 'Yes' to (d) above, please confirm that concerns were addressed and rectified? Yes ☐ No ☐

ASCENT™ UNDERWRITING

Privacy Questionnaire

4 Third Party Service Providers

If you outsource any element of your network please provide details

a. Web hosting — (Name of Service Provider)

b. Security services — (Name of Service Provider)

c. ASP — (Name of Service Provider)

d. Data processing — (Name of Service Provider)

e. Point of sale/Payment card processing — (Name of Service Provider)

f. Other — (Detail of service) — (Name of Service Provider)

5 Network Security

a. Do you employ a Chief Privacy Officer or Chief Information Officer who has responsibility for meeting your worldwide obligations under privacy and data protection laws? Yes ☐ No ☐

b. Does your security and privacy policy include mandatory training for all employees? Yes ☐ No ☐

c. Are all employment positions analysed and employees assigned specified rights, privileges and unique user ID and passwords, which are changed periodically? Yes ☐ No ☐

d. Do you have user revocation procedures on user accounts and inventoried recovery of all information assets following employment termination? Yes ☐ No ☐

e. Do you conduct regular reviews of your third party service providers and partners to ensure that they meet your requirements for protecting sensitive information in their care? Yes ☐ No ☐

f. Do you have antivirus software on all computer devices, servers and networks which are updated in accordance with the software providers' recommendations? Yes ☐ No ☐

g. Do you have firewalls and intrusion monitoring detection in force to prevent and monitor unauthorized access? Yes ☐ No ☐

h. Do you ensure that all wireless networks have protected access? Yes ☐ No ☐

i. Do you have access control procedures and hard drive encryption to prevent unauthorized exposure of data on all laptops, PDAs, smartphones and portable devices? Yes ☐ No ☐

j. Do you encrypt all sensitive information that is transmitted within and from your organization? Yes ☐ No ☐

k. Is all sensitive and confidential information stored on your databases, servers and data files encrypted? Yes ☐ No ☐

If you answer 'No' to questions (h), (i), (j), (k) above, please provide details below, briefly describing the nature of the unprotected information and what security measures are in force to protect this information in the absence of encryption.

6 Information and Data Management

a. Does your information asset programme include a data classification standard (e.g. public, internal use only, confidential)? Yes ☐ No ☐

b. Do you post a privacy policy on your website which has been reviewed by a qualified lawyer? Yes ☐ No ☐

c. Does your privacy policy include a legally reviewed statement advising users as to how any information collected will be used, and for what purposes? Yes ☐ No ☐

6 Section 6 Continued

d. Do you have procedures in force for honouring the specific marketing "opt-out" requests of your customers that are consistent with the terms of your published privacy policy? Yes ☐ No ☐

e. Do you have procedures in place to monitor the period for which customer data is held and have processes for deleting this information at the end of that period? Yes ☐ No ☐

f. Do you have procedures in force for deleting all sensitive data from systems and devices prior to their disposal from the company? Yes ☐ No ☐

g. Is all information held in physical form (paper, disks, CD's etc) disposed of or recycled by confidential and secure methods, which are recognized throughout the organisation? Yes ☐ No ☐

h. Do you keep an incident log of all system security breaches and network failures? Yes ☐ No ☐

i. Have you identified all relevant regulatory and industry compliance frameworks? Yes ☐ No ☐

If 'Yes' please provide details:

Compliant		**Date of latest audit**
Gramm-Leach Bliley Act of 1999	Yes ☐	
Health Insurance Portability & Accountability Act of 1996	Yes ☐	
Payment Card Industry (PCI) Data Security Standard	Yes ☐	

If 'Yes' What level requirement 1 ☐ 2 ☐ 3 ☐ 4 ☐

Other (please provide details)

7 Claims and Circumstances

During the last three years have you:

a. Sustained any unscheduled or unintentional network outage, intrusion, corruption or loss of data? Yes ☐ No ☐

b. Received notice or become aware of any privacy violations or that any data or personally identifiable information has become compromised? Yes ☐ No ☐

c. Notified any customers that their information may have been compromised? Yes ☐ No ☐

d. Received any injunction(s), lawsuit(s), fine(s), penalty(s) or sanction(s)? Yes ☐ No ☐

e. Become aware of any circumstance or incident that could be reasonably anticipated to give rise to a claim against the type of insurance(s) being requested in this application? Yes ☐ No ☐

If 'Yes' to any questions within this section, please provide full details:

ASCENT™
UNDERWRITING

Privacy Questionnaire

IMPORTANT – CyberPro Policy Statement of Fact

This questionnaire is supplementary documentation and forms part of the application submission for insurance.

The undersigned is an authorized principal, director, risk manager or employee of the applicant and certifies that reasonable inquiry has been made to obtain the answers herin which are true, correct and complete to the best of his/her knowledge and belief. Such reasonable inquiry includes all necessary inquiries to fellow principals, directors, risk managers, or employees to enable you to answer questions accurately.

Name	Position
Print & Sign	Date

Additional Notes