PRINCIPIA UNDERWRITING

Network Security Application Form

Note that this application is for claims made policy; this means the policy will only apply to claims made against the insured and reported in writing during the specified policy period.

The form must be signed and dated by a director of the company, and any responses to the questions below that change, after the form has been signed and submitted but prior to inception of a policy being granted on the basis of the information contained within, must be notified to underwriters immediately. Failure to do so may invalidate your coverage.

Section 1 – General Information

1. Company or Trading Name:

2. Names of Subsidiaries/Additional Insured to be covered under this policy:

3. Address:

4. Website Address:

5. Total No. of Staff:

6. Year Established

7. Business description:

PRINCIPIA
UNDERWRITING

Network Security Application Form

8. Do you provide any of your customers with a managed hosting service, including websites, emails, remote access/ cloud based services:

Yes ☐ No ☐

9. Mergers or Acquisitions in the last 3 years or planned in the next 12 months:

9. Gross Revenue:

	Past Year (USD)	Current Year (USD)	Next Year (USD)
US/Canada			
Rest of World (ROW)			
Total			

10. Revenue derived from online activities

11. Do you use independent contractors/sub contractors Yes ☐ No ☐ N/A ☐

12. Revenue attributable to sub contractors

13. % of work carried out by sub contractors

14. Do you always use a written contract with contractors/sub contractors:

Yes ☐ No ☐

15. If 'Yes' does the written contract include a provision to the effect that any liability arising from the work of contractors/sub contractors will require them to indemnify you:

Yes ☐ No ☐

16. Do you require contractors/sub contractors to carrier E&O Insurance:

Yes ☐ No ☐

17. Do you outsource any parts of your IT operation

Yes ☐ No ☐

18. If 'Yes' please detail

IT outsource service provider	Service

19. Have you identified all relevant regulatory and industry compliance frameworks that are applicable to the organisation:

Gramm-Leach Bliley Act of1999	Yes ☐	No ☐	N/A ☐
HIPAA	Yes ☐	No ☐	N/A ☐
PCI	Yes ☐	No ☐	N/A ☐
Other	Yes ☐	No ☐	N/A ☐

If 'Yes' to other please describe:

20.. Please indicate the nature of & volume of records processed

Customers names and addresses:	☐
Credit or debit card numbers:	☐
Social security numbers:	☐
Medical records/personally identifiable health records:	☐
Financial records:	☐
Other personally identifiable sensitive information:	☐:
Volume of records processed:	

20. Level of PCI compliance: 1.☐ 2.☐ 3.☐ 4.☐

PRINCIPIA
UNDERWRITING

Network Security Application Form

22. Date of last PCI audit:

21. Is your information as identified in **Q20.** stored on a web facing server:

Yes ☐ No ☐

22. Can sensitive and confidential information including personally identifiable information be downloaded onto mobile devices (e.g. blackberrys) Yes ☐ No ☐

23. Is all sensitive and confidential information within your organisation encrypted using industry grade mechanisms whilst:

At rest	Yes ☐ No ☐
In transit	Yes ☐ No ☐
On portable devices	Yes ☐ No ☐
On backup tape or similar storage devices	Yes ☐ No ☐

24. Do you use firewall technology at all relevant connection points and on all terminals and relevant network devices across you network to prevent unauthorised access. Yes ☐ No ☐

25.. Have you kept the settings as per the manufactures standards for the firewall technology:

Yes ☐ No ☐

If 'No' please elaborate on the changes:

26. Do you use antivirus software on all computers, laptops, portable devices and servers

Yes ☐ No ☐

27. How often are virus definitions and anti-virus patches updated

Live, as released	Yes ☐ No ☐
As per manufactures guidelines	Yes ☐ No ☐
Within 30 days	Yes ☐ No ☐
Greater than 30 days after release of update	Yes ☐ No ☐

PRINCIPIA UNDERWRITING

Network Security Application Form

28. How often is software updated in respect to all other software patches/updates

Live, as released	Yes ☐ No ☐
As per manufactures guidelines	Yes ☐ No ☐
Within 30 days	Yes ☐ No ☐
Greater than 30 days after release of update	Yes ☐ No ☐

29. Do you operate intrusion detection software: Yes ☐ No ☐

If 'Yes' how often are the logs reviewed:

Daily ☐ Weekly ☐ Monthly ☐ Other ☐

30. Do you back up your systems Yes ☐ No ☐

31. If 'Yes' on what basis?

Daily	☐
Weekly	☐
Monthly	☐
Other	☐

32. Are the backups stored offsite, or in a fireproof safe on site. Yes ☐ No ☐

33. If 'No' are they stored on site in a fireproof safe Yes ☐ No ☐

33. Do you have a disaster recovery plan (DRP), Yes ☐ No ☐

34. If 'Yes' does it cover the following

Key persons	Yes ☐ No ☐
Mirrored sites/redundant servers	Yes ☐ No ☐
Alternative physical locations	Yes ☐ No ☐
Timelines for recovery	Yes ☐ No ☐
Loss of outsourced IT provider	Yes ☐ No ☐
Network breach response plan	Yes ☐ No ☐

35. How often is the DRP tested

Annually	☐
Bi-Annually	☐
Quarterly	☐
Other	☐

PRINCIPIA
UNDERWRITING

Network Security Application Form

36. Do you have business continuity plan (BCP), Yes ☐ No ☐

37. If 'Yes' please briefly describe the contingency plan in place to minimise any network interruption caused by any unplanned downtime

38. What is the dependency of your business on access to data and business applications:

High – any interruption will have a significant and immediate effect Yes ☐
Moderate – no material impact for up to the first 12 hours Yes ☐
Low – no material impact for up to the first 24-48 hours Yes ☐

39. In the last 24 months have you been subject to an IT audit. Yes ☐ No ☐

40. As a result of the audit were any red or amber flags raised Yes ☐ No ☐

41. If 'Yes' please provide a brief synopsis of the issues raised

42. Have all recommendation from the audit now been met Yes ☐ No ☐

43. have you ever subjected your systems or offices to penetration testing/social engineering exercises. Yes ☐ No ☐

44. If 'Yes' please summarise the outcome

PRINCIPIA
UNDERWRITING

Network Security Application Form

45. Do you provide training to your employees where relevant , to those that deal with sensitive customer data as part of their employment Yes ☐ No ☐

46. Do you have a written procedure for employees in relation to internet and email and system usage Yes ☐ No ☐

43. Do you have a procedures in place to ensure that users update their passwords every 60 days and that passwords are not repeated and contain a minimum of 9 characters consisting of a mix of alpha and numeric characters in both upper and lower case. Yes ☐ No ☐

44. Do you provide remote access to your system for your employees Yes ☐ No ☐

45. Where remote access is possible do you require a minimum of three factor authentication.

Yes ☐ No ☐

46. Do you have a Chief Information Officer or a Board level representative responsible for information security Yes ☐ No ☐

47. Do you have an asset classification programme including data (e.g. public, internal use only)
Yes ☐ No ☐

48. Do you have procedures in place for the destruction, sale or refurbishment of hardware, and storage devices used to hold confidential information (e.g. external hard drives)

Yes ☐ No ☐

49. Do you have in place procedures to deal with California Senate Bill 1386 or similar laws pertaining to disclosure requirements following a security breach. Yes ☐ No ☐

50. Do any of your websites utilise cookie tracking/user data aggregation technology.
Yes ☐ No ☐

51. Regarding the risks to which this proposal form relates, in the last 5 years after enquiry:-

a) have you suffered any losses or had any claims made against the Company

Yes ☐ No ☐

b) are you aware of any circumstances which may give rise to a loss or claim against the Company

Yes ☐ No ☐

c) has the Company suffered or received any complaints involving any breach of security, data loss or breach of privacy

Yes ☐ No ☐

d) has the Company or any of its partners or directors been found guilty of any criminal, dishonest or fraudulent activity or been investigated by any regulatory body

Yes ☐ No ☐

This questionnaire completed by:

Name			
Title		Date	
Signature			

ALL INFORMATION PROVIDED WILL BE HELD IN CONFIDENCE.