RESET

Utica National Insurance Group®

Named Insured: ______________________________

Policy Number: ______________________________

Cyber Suite Questionnaire

The Data Compromise Liability Coverage, Network Security Liability Coverage, And Electronic Media Liability Coverage* Apply On A Defense Within Limits Basis. Any Defense Costs Paid Will Reduce The Available Limit Of Insurance And May Exhaust It Completely. Defense Costs Will Also Be Applied Against The Deductible. In The Event That The Limit Of Insurance Is Exhausted, We Will Not Be Liable For Further Defense Costs Or For Any Damages Or Judgments.

** Not applicable in New York*

Select a Limit and Corresponding Deductible

Limit	Deductible
□ $50,000**	$1,000
□ $100,000	$1,000
□ $250,000	$2,500
□ $500,000	$10,000
□ $1,000,000	$10,000

*** Not available in New Hampshire or New York*

I. Complete This Section for $500,000 or $1,000,000 Limit

If the answer to question **1.** is "yes", higher limits are not available. In addition, if you answer "No" to three or more of the remaining questions, higher limits are not available.

1. Have you, at any time during the past 36 months, experienced a cyber incident (hacking, intrusion, malware infection, fraud loss, breach of personal information, extortion, etc.) that cost you more than $10,000 or experienced a lawsuit or other formal dispute (with either a private party or government agency) arising from a cyber incident? □ Yes □ No

2. Do you use up-to-date anti-virus and anti-malware protection on all of your endpoints (desktops, laptops, servers, etc.)? □ Yes □ No

3. Are all of your internet access points secured by firewalls? □ Yes □ No

4. Do you restrict employees' and external users' IT systems privileges and access to personal information on a business-need-to-know basis? □ Yes □ No

5. Do you perform backups of business critical data on at least a weekly basis? □ Yes □ No

6. Do you encrypt all of your mobile devices (laptops, flash drives, mobile phones, etc.) and confidential data? □ Yes □ No

II. Complete This Section for Limits Greater Than $1,000,000

7. How many of the following devices do you currently have deployed?
Servers: ______ Desktops: ______ Laptops: ______ Mobile Phones/Devices: ______

8. How many individual people (employees, customers, etc.) do you currently store or maintain (either yourself or using third parties) information about? __________

9. Do you process or store personal information or other confidential information for other businesses or organizations? □ Yes □ No

10. For each vendor that processes or stores personal information for you, do you have a written agreement that makes the vendor financially responsible for the consequences of a cyber-attack or data breach? □ Yes □ No

11. Do you require service providers to demonstrate adequate security? □ Yes □ No

12. Do you have a written organization-wide privacy and security policy? □ Yes □ No

13. Do you have a document retention and destruction policy? □ Yes □ No

14. Have you implemented a policy requiring multiple internal parties to confirm authorization before making payments (including wire and ACH transfers) in excess of $10,000? □ Yes □ No

15. Does each user of your system have a separate individual account? □ Yes □ No

16. Do you have a formal process (which includes identification, tracking, and monitoring) in place for properly bringing servers, desktops, laptops and other digital assets into service and a formal process (which includes removal from the network, deleting from inventory and secure wiping of sensitive data) for properly removing those assets from service? □ Yes □ No

17. If you accept payment (credit and debit) cards, do you comply with Payment Card Industry Data Security Standards? □ Yes □ No

18. If you handle health information, do you comply with HIPAA and the HITECH act?) □ Yes □ No

19. Do you have a designated Chief Information Officer or other person responsible for information and systems security? □ Yes □ No

20. Have you identified and secured personal and other highly confidential information for which you are responsible? □ Yes □ No

21. Do you update and patch critical IT-systems and applications on at least a monthly basis? □ Yes □ No

22. Have you implemented the use of long and complex passwords or another secure account access methodology such as multifactor identification or universal identification? □ Yes □ No

23. Are all Internet-accessible systems (for example, web-, email-servers) segregated (for example, within a DMZ or at a 3rd party provider) from your trusted network? □ Yes □ No

24. Do you use intrusion detection hardware or software or otherwise monitor your network and identify security events? □ Yes □ No

25. Do you provide awareness training for employees in data privacy and security issues (including legal liability issues and phishing)? □ Yes □ No

26. Do you delete system access, accounts and associated rights after termination of users (including employees, temporary employees, contractors and vendors)? ☐ Yes ☐ No

27. Do you (yourself or by engaging an outside vendor) regularly scan critical systems for security vulnerabilities? These scans may include security and penetration testing. ☐ Yes ☐ No

28. If you perform backups of business critical data on at least a weekly basis, is the backup stored offsite in a secure location? ☐ Yes ☐ No

29. If you perform backups of business critical data on at least a weekly basis, do you test your restore process on at least a monthly basis? ☐ Yes ☐ No

30. Do you have a business continuity management or disaster recovery plan in place? ☐ Yes ☐ No

31. Do you have an incident response plan (for cyber-attacks and data breaches) that identifies an incident response team? ☐ Yes ☐ No

32. Do you have a process in place to review all advertising and other content prior to publication? ☐ Yes ☐ No

FRAUD WARNINGS

FOR THE FOLLOWING STATES:

DISTRICT OF COLUMBIA - WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the applicant.

KENTUCKY and PENNSYLVANIA - Any person who knowingly and with intent to defraud any insurance company or other 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 subjects such person to civil and criminal penalties.

MARYLAND - Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

OHIO - Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

FOR ALL OTHER STATES EXCEPT NEW YORK:

Any person who knowingly presents a false claim or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison, and denial of insurance benefits.

FOR NEW YORK - Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim 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 shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

Person Completing Form: ______________________ Title: ______________________

Signature(s): ______________________ Date: ______________________

I/We HEREBY DECLARE that the above statements and particulars are true to the best of my/our knowledge and that I/we have not suppressed or misstated any facts, and I/we agree that this questionnaire shall be the basis of the coverage issued by the company providing this insurance, and shall be deemed attached to and part of the policy. It is also acknowledged that the applicant is obligated to report any changes in the information provided herein that occur after the date of signature but prior to the effective date of coverage.