Cyber Liability - Supplemental Application

Instructions: Please answer all questions. This information is required to make an underwriting and pricing evaluation. Your answers hereunder are considered material to that evaluation. **Items in bold/underlined are defined in an attached appendix.**

Applicant Name: _____

1. Gross Operating Expenses? _____ *(General fund expenses less capital projects)*

2. What sensitive information do you handle, manage, store, destroy, or otherwise control? (Please check all that apply and provide approximate number of records)

☐ Social Security Numbers	_____	☐ Medical Records	_____
☐ Credit/Debit Card Numbers	_____	☐ Healthcare Records	_____
☐ Drivers License Numbers	_____	☐ Credit History and Ratings	_____
☐ Government ID Numbers	_____	☐ Intellectual Property of Others	_____
☐ Financial Account Numbers	_____	☐ Other: _____	_____

3. Do you have a process to manage access to sensitive information which includes timely account termination? _____
   a. If yes, please describe:

4. Do you have a security program that prohibits, tracks, and logs unauthorized access to your computer systems? _____

5. Do your external interfacing computer systems (i.e. public websites, mobile devices) utilize firewall & intrusion detection/prevention systems? _____
   a. If yes, please identify the technologies used:

6. Does your computer system (including e-mail & remote access) use security products that address the detection of common **malware** and/or malicious activity? _____
   a. If yes, please identify the technologies used:

7. Do you have a scheduled reoccurring vulnerability assessment program? _____

8. Do you have a **patch** management program in place? _____
   a. If yes, please describe:

9. Do you have encryption tools to ensure integrity & confidentiality of sensitive information on removable media, such as USB devices, memory sticks, CDs, DVDs, etc.? _____

   a. If yes, please identify the technologies used:

10. Do you have a thorough Information Security Policy & Privacy Policy that is updated periodically and consistently enforced? _____

    a. If yes, how frequently is it reviewed and/or updated? _____
    b. If yes, has the policy been reviewed by a qualified attorney? _____
    c. If yes, does it comply with legislative, regulatory, and/or contractual privacy requirements? _____
    d. If no, please describe your organization's plans to create/update such a policy:

11. Do you provide awareness training for employees on data privacy and security issues? _____

    a. If yes, please describe the type, method and frequency of training:

12. In the event that data is compromised or your systems are breached, do you have a disaster recovery plan in place? _____

13. Are there certain departments that operate on their own domain not managed by the County information services staff? _____

    a. If yes, which departments?

14. Do you (or a third party on your behalf) process, store, or handle credit card transactions? _____

    a. If yes, are you/they in compliance with **Payment Card Industry Data Security Standards**? _____
    b. If yes, what is your/their required level of compliance? _____
    c. If yes, are these transactions encrypted? _____ Encryption type? _____
    d. If using a third party, please answer the following questions:

       i. Describe how payment card data is captured and transferred. (i.e. are point-of-sale systems segragated from other county networks, is data sent via direct link or via the public internet, etc.)

       ii. What type of review is done on the provider to certify they have similar controls and protocols discussed within this application?

15. If you outsource any part of your network, computer system, or information security functions, please provide vendor name below:

    a. **Data Center Hosting Vendor** _____
    b. **Managed Security Vendor** _____

c. **Data Processing Vendor** _____

d. **Application Service Provider** _____

e. **Offsite Backup & Storage Vendor** _____

16. Do you require vendors who handle your data processing/hosting functions to show adequate security of their computers? _____

    a. If yes, please indicate method of verification:

17. Do you currently use a cloud service provider? _____

    a. If yes, provide the provider name(s). _____

    b. What services do they provide (**IaaS - Infrastructure as a Service, PaaS - Platform as a Service, SaaS - Software as a Service**)? _____

    c. Are the service networks public, private, or a hybrid? _____

18. Have you had any occurrences, claims, or losses related to a failure of security of your computer system in the past five (5) years? _____

    a. If yes, please attach a detailed loss run with description of the loss.

19. Has anyone filed a suit or made a claim against you with regard to invasion or interference with rights of privacy or wrongful disclosure of Confidential Information? _____

    a. If yes, please describe:

20. Are you aware of a situation or circumstance which could result in a claim against you with regard to issues related to the cyber coverage you are seeking? _____

    a. If yes, please describe:

Date Completed: _____

Completed by: _____

Title & Department: _____

Questions: 801.307.2113
Submit to: UCIP: sonya@ucip.utah.gov

Appendix - Definition of Terms

Malware - Malicious software or computer code used to disrupt computer operation, gather sensitive information, or gain access to private systems.

Patch - Software designed to update, fix, and/or improve your computer on a periodic basis. Includes patches/fixes for: security vulnerabilities, bugs, removing outdated software, improving usability or performance, etc.

Payment Card Industry Data Security Standards - for more detailed information please visit the website below: https://www.pcisecuritystandards.org/security_standards/index.php

Data Center Hosting Vendor (a.k.a Cloud Provider) - Service provider who has their own off-site facility to house computer systems which store your organization's data.

Managed Security Vendor - Service provider who oversees the organization's network and information security. Functions may include: monitoring and management of intrusion detection systems/firewalls, overseeing patch management and upgrades, data storage, handling integrity and confidentiality protection, system monitoring and data analysis, performing security assessments and security audits, and responding to emergencies.

Data Processing Vendor - Service provider who produces, compiles, retrieves, and/or maintains data on behalf of your organization. Examples include: data warehouse management, maintaining employment records, filing payroll tax returns, computing and preparing payroll checks, etc.

Application Service Provider - Service provider who employs the use of an internet based application to store organizational data. Unlike an application that is on your individual computer (i.e. Microsoft Word), the application is accessed via the internet and stores data inputted by your organization.

Offsite Backup & Storage Vendor - Service provider who stores a "copy" of your organization's data on their own off-site computer system or stores physical backup media (i.e. tape drives). Data is created and stored on a local computer or server, however the service provider makes routine copies of this data in the event that your local storage is compromised or damaged.

Infrastructure as a Service (IaaS) - The cloud provider provides the hardware/computers (physical or virtual), storage, and networking components to your organization. They own the components and are responsible for housing, running, and maintaining it.

Platform as a Service (PaaS) - The cloud provider provides a virtual computing platform (i.e. operating system, programming language execution environment, database, web server) to your organization.

Software as a Service (SaaS) - The cloud provider provides an application(s) to your organization. They own the application and are responsible for housing the application and user data entered (see Application Service Provider). Often referred to as "software-on-demand" and utilizing it is akin to renting software rather than buying it.