citycounty insurance services
cisoregon.org

*CIS – Tier Two & Tier Three Cyber Coverage Application**

Name of Applicant:

Requested Date of Coverage:

TIER TWO LIMIT REQUEST OPTION:

☐ $200,000**

**** Coverage Limit is excess of the Tier One $50,000 provided under the CIS Property Coverage Agreement.**

TIER THREE (COMMERCIAL EXCESS) ADDITIONAL LIMIT REQUEST OPTIONS:

☐ $250,000 ☐ $750,000

A. CYBER PLANNING

1. Does your entity have an adopted cyber security policy than includes?
   a) Table-top drill annually — YES ☐ NO ☐
   b) Password strategy — YES ☐ NO ☐

   If YES, provide a brief explanation of your cyber security policy: _____

   CIS also offers a **sample cyber security policy**
2. Do you have a policy in place to prevent repeated attempts of unauthorized access to your network and publicly accessible applications? YES ☐ NO ☐
3. Do you have a Personal Identifiable Information (PII) policy in place? YES ☐ NO ☐

B. ASSESSMENT

1. Do you collect social security numbers? YES ☐ NO ☐
   If YES, number of social security numbers: _____
2. Do you collect credit/debit card numbers? YES ☐ NO ☐
   If YES, number of credit/debit card numbers: _____
3. Do you collect bank account details? YES ☐ NO ☐
   If YES, number of bank account details: _____
4. Do you collect driver license numbers? YES ☐ NO ☐
   If YES, number of driver license numbers: _____
5. Do you collect protected health information? YES ☐ NO ☐
   If YES, number of protected health information: _____
6. Do you collect other personal identifying information? YES ☐ NO ☐
   Explain if YES: _____
7. Approximate number of credit/debit card transactions in a year: _____
8. Number of PII records stored: _____
9. Number of employees: _____

10. Do you offer cyber services for a fee? (ISP, data storage, backup services)? YES ☐ NO ☐

Explain if YES: _____

11. Do you comply with Payment Card Industry Data Standards? YES ☐ NO ☐

12. Website URL: _____

13. Population: _____

14. Position responsible for data security (internal/external) Position Title: _____

15. Is firewall internal or network perimeter? _____

16. Has your entity had any cyber breaches of data or losses that might cause a claim? Please include incidences such as data breaches or network outages causing significant disruption, even if a claim was not made. YES ☐ NO ☐

Explain if YES: _____

C. MITIGATION

1. Does your entity include multi-factor authentication on the following?
   a) VPN YES ☐ NO ☐
   b) Email YES ☐ NO ☐
   c) Remote access (via RDP or other web-based access) YES ☐ NO ☐
   d) Privileged account access YES ☐ NO ☐
2. Does your entity deploy endpoint protection, detection and with 24/7/365 response across all desktops and servers on the company network? YES ☐ NO ☐
3. Does your entity include the following in your back-ups?
   a) 3 copies; 2 offsite (geo-diverse), 1 onsite (source) YES ☐ NO ☐
   b) At least one copy stored offline or in a cloud service designed for this purpose YES ☐ NO ☐
   c) Tested at least twice a year YES ☐ NO ☐
   d) Protected with antivirus or monitored on a continuous basis YES ☐ NO ☐
   e) Encrypted YES ☐ NO ☐
4. Does your entity perform semi-annual phishing testing? YES ☐ NO ☐
5. Does your entity perform annual remote penetration testing? YES ☐ NO ☐
6. Does your entity have critical and high severity patches installed within 30 or fewer days? YES ☐ NO ☐
7. Does your entity plan include adequate measures in place to upgrade end-of-life software? YES ☐ NO ☐
8. Do you encrypt all mobile devices with PII (laptops, notebooks, PDAs, flash drives)? YES ☐ NO ☐
9. Are there pre-authorization controls for all programmers and operators? YES ☐ NO ☐

D. TRAINING

1. Does your entity require employees to be trained in the following?
   a) Cyber security basics (CIS Learning Management session) YES ☐ NO ☐
   b) Finance training on Fraudulent Instruction risk controls YES ☐ NO ☐
2. Do you have an active phishing training? YES ☐ NO ☐

E. DISCOVERY

CIS will arrange for a firm named VC3 to contact you if you qualify for Tier Two or Tier Three. VC3 will perform technical and verbal assessment. **The cost of the discovery is $500** and paid by the member to qualify for coverage. Results are kept confidential.

F. CONTACT INFORMATION

Name: _____ Email Address: _____

Date: _____ Signature: _____

PLEASE BE AWARE THAT ALL RISK CONTROLS ASKED ABOUT ABOVE MUST BE IN PLACE OR APPLICATION WILL BE DECLINED.

FOR TECHNICAL QUESTIONS REGARDING THIS APPLICATION PLEASE EMAIL: cybersecurityquestions@cisoregon.org

*EXEMPT FROM PUBLIC RECORD REQUESTS in accordance with ORS 192.345(23) and generally accepted government auditing standards to avoid disclosure of security weaknesses.

citycounty insurance services
cisoregon.org

Supplement to Application

The “Discovery Assessment” can be completed any time before June 1, 2022, for Tier Two or Tier Three cyber coverage. The member’s cost is $500 (see Section E. below).

A. CYBER PLANNING

Question 1:

a) A table-top drill must be completed by December 30, 2022. CIS will have a sample table-top drill with CISA at the CIS Annual Conference on August 24, 2022.

b) A password strategy is required. The response to this question must be “YES” to qualify for coverage.

Question 2: A cyber security policy is required. The response to this question must be “YES” to qualify for coverage.

Question 3: A PII policy is required. The response to this question must be “YES” to qualify for coverage.

B. ASSESSMENT

Question 10: CIS cannot offer coverage if your entity offers internet or other cyber services as a service to third parties. A “YES” answer disqualifies your entity from CIS coverage.

Question 11: CIS does not offer Payment Card Industry coverage. Nevertheless, we expect a “YES” answer.

Question 16: Prior claims may disqualify your entity from obtaining coverage. A “YES” answer will prompt a discussion with CIS. A meeting with CIS and IT staff may be necessary to ensure vulnerabilities are corrected.

C. MITIGATION

Question 1:

a) Remote VPN access must have MFA by December 30, 2022. (A “NO” answer must come with a commitment date to qualify for coverage.)
b) Remote email access must have MFA by June 1, 2022. Office 365 includes MFA for email. (A “YES” answer is required.)
c) Remote Network Level Authentication access (via RDP or other web-based access) must have MFA by June 1, 2022. (A “YES” answer is required.)
d) Remove access to privileged account access, or IT access must have MFA by June 1, 2022. (A “YES” answer is required.)

Question 2: CIS prefers an outside monitoring service for EDR. Microsoft is acceptable (see link below for information). Internal EDR monitoring will require a meeting with CIS and your IT department. CIS will postpone the activation of any monitoring service until December 30, 2022. You may consider Sentinel 1 through a firm such as Loadstone. A "NO" answer must come with a commitment date to qualify for coverage.

Multifactor authentication for Microsoft 365 - Microsoft 365 admin | Microsoft Docs

Question 3:

a) Geo-diverse – we prefer out-of-state back-ups but will accept in-state if in a different county. (A "YES" answer is required.)
b) Back-ups must not be "connected" in any way to your network — there must be "gates" between the network and back-ups (A "YES" answer is required.)
c) Tested twice a year
d) Back-ups must be protected with an antivirus software. (A "YES" answer is required.)
e) Back-ups must be encrypted. (A "YES" answer is required.)

Question 4: Semi-annual phishing testing is a minimum requirement. (A "YES" answer is required and means you commit to test during the year.)

Question 5: Annual remote penetration testing is required. (A "YES" answer is required and means you commit to test during the year.)

Question 6: Patches are required (A "YES" answer is required and means you will install patches during the year.)

Question 7: A plan is required to protect/upgrade end of life software that you have control over. (A "YES" answer is required.) For software for which you have no control over, we recommend you work with the software vendor to require this action.

Question 8: Encryption of all mobile devices is required. (A "YES" answer is required.)

Question 9: Programmers and operators have pre-authorized controls. (A "YES" answer is required.)

D. TRAINING

Question 1: Training is available in our online CIS Learning Center. Other similar training is acceptable. Police Officer training in cyber liability satisfies this requirement. (A "YES" answer is required for 1. a. and b.)

E. DISCOVERY ASSESSMENT

CIS will arrange for a cybersecurity assessment through VC3. Members can receive this assessment at any time for $500. The Discovery Assessment must be completed prior to June 1, 2022, for Tier Two or Tier Three coverage.