



CIS – Tier Two & Tier Three Cyber Coverage Application*

(Min. \$250,000 Excess Crime Coverage required –
complete separate CIS Excess Crime Coverage Application if applicable)

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 Cyber Security Coverage Agreement.

TIER THREE (COMMERCIAL EXCESS) ADDITIONAL LIMIT REQUEST OPTIONS:

\$250,000 \$500,000 \$750,000 \$1,000,000

A. CYBER PLANNING

1. Does your entity have an adopted cyber security policy that includes? ***REQUIRED**

a) Table-top drill annually YES ___ NO ___

b) Password strategy ***REQUIRED** YES ___ NO ___

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? ***REQUIRED** 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) At least one offsite (geo-diverse) ***REQUIRED** 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) ***REQUIRED** YES ___ NO ___
 - b) Finance training on Fraudulent Instruction risk controls ***REQUIRED** YES ___ NO ___
2. Do you have an active phishing training? YES ___ NO ___

E. CONTACT INFORMATION

Name:

Email Address:

Date:

Signature:

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.

Supplement to Application

A. CYBER PLANNING

Question 1: A cyber security policy is required. CIS provides a sample [Cyber Security Policy](#).

- a) A table-top drill is recommended annually and included in the CIS sample policy, but no longer required for coverage.
- b) A password strategy is required. The response to this question must be “YES” to qualify for coverage.

Question 3: A PII policy is required. This requirement has been a state law for many years.

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.

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: MFA for VPN, web-based email, and web-based remote access to network resources is recommended.

Question 2: An outside monitoring service for EDR is recommended.

Question 3: Back-ups

- a) Geo-diverse – CIS prefers out-of-state back-ups but will accept in-state if in a different county or a couple of miles away (A “YES” response is required.)
- b) Back-ups should not be “connected” in any way to your network — there should be “gates” between the network and back-ups.
- c) Tested twice a year.
- d) Back-ups should be protected with antivirus software.
- e) Back-ups should be encrypted.

Question 4: Semi-annual phishing testing is recommended.

Question 5: Annual remote penetration testing is recommended.

Question 6: Patches are recommended.

Question 7: A plan is recommended to protect/upgrade end-of-life software that you have control over. We recommend you work with the software vendor to require this action.

Question 8: Encryption of all mobile devices is recommended.

Question 9: Programmers and operators have pre-authorized controls.

D. TRAINING

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