



SMALL AGENCY CYBER LIABILITY INSURANCE OVERVIEW

POLICY YEAR 2024-2025

For policy year 2024-2025, the Department of Enterprise Services, Office of Risk Management (ORM) has purchased cyber liability insurance from Alliant Insurance Services for small agencies. This insurance is available only to agencies who do not participate in the Alliant Property Insurance Program (APIP). The Small Agency Cyber Liability Insurance Pool provides the following coverage:

- This policy provides covered individual agencies with limits of \$1,000,000 per claim / \$5,000,000 aggregate for most coverages. See below for specific coverages.

This document provides an overview of the cyber liability insurance policy, provides answers to frequently asked questions, explains specific cyber liability coverages and limits, and defines key terminology. The actual policy, which is available from ORM, contains additional descriptions, definitions, and exclusions.



POLICY SUMMARY 2024-2025

INSURANCE COMPANY:	Obsidian Insurance Company
A.M. BEST RATING:	A- (Excellent) Financial Size VII (\$1B to \$1.25B) as of 11/10/22
STATE COVERED STATUS:	Non-Admitted
Coverage Form:	BMS Municipal Cyber Program
Policy Total Limits:	\$5,000,000
Aggregate Limit	\$5,000,000
Aggregate per Member	\$1,000,000
Data Breach Incident Response	\$1,000,000
Network Security, Privacy and Data Breach Liability	\$1,000,000
Regulatory Liability	\$1,000,000
PCI Fines and Assessments	\$1,000,000
Data Restoration	\$1,000,000
Network (Business) Interruption and Recovery	\$1,000,000
Cyber Extortion	\$1,000,000
Media Liability	\$1,000,000
Dependent Business Interruption per Member	\$250,000
Ransomware	Included
Social Engineering	\$250,000
Biometric Data	Excluded
Retention	\$250,000 per Member 12 Hours for Business Interruption 24 Hours for Contingent Business Interruption Losses

Policy period: 07/01/2024 – 07/01/2025

Policy type: Claims Made (e.g., covered incidents must occur and be reported within the policy period)

Retroactive Date: Full Prior Unknown Acts



FREQUENTLY ASKED QUESTIONS

The following responses to common questions reflect the high points of our current Small Agency Cyber Liability Insurance policy. Please contact the ORM if you need more detailed information about this policy.

1. What is cyber liability?

Cyber liability includes breach response, first and third-party risks associated with the use of computer hardware and software systems, the Internet, networks, mobile computing devices, and other electronic information assets. Examples include:

- Data privacy issues
- Virus/malicious software (malware) transmission to a third party
- Business interruption and data recovery
- Regulatory defense and fines
- Cyber extortion
- Website or media misuse
- Infringement of intellectual property

2. What specific insurance coverages does the policy provide?

To understand how cyber liability insurance is structured, think about your homeowner's insurance policy. You have first-party damages insurance that covers things like fire and water damage, and you have third-party liability coverage in case your tree falls on your neighbor. Cyber liability insurance has first-party damage coverage and third-party liability coverage. In this case, the first-party is the state and the state's infrastructure and the third-party would be other citizens whose information we have in our computer systems in the form of data.

For example, we have a data breach of personal information as defined by RCW 42.56.590, and it involves the theft of 200,000 citizen records. Per this regulation, the agency that experienced this incident is required to give notice to the 200,000 people. The cost to do that would be a first-party damage. Using an estimate of \$3 per record, we have a total cost of \$600,000. The agency would pay the first \$250,000 as a deductible and the cyber liability insurance would pay the remaining \$350,000.

If the breach causes damage to citizens, and they file a tort claim against the state, we could have a third-party liability. In this case, the cost per record goes up significantly.

Please review the Cyber Liability Insurance Coverages and Limits below with this in mind.



3. What is the deductible for the Small Agency cyber liability insurance policy?

The deductible amount is \$250,000.00.

4. How do we know the cyber liability policy will pay out when we need it?

The state requires our insurance broker to offer us insurance only from insurance firms with a rating of "A" or better. This designation refers to the international ratings by AM Best.

5. Does the small agency cyber liability insurance policy cover all state agencies?

No, only small agencies that do NOT participate in the Alliant Property Insurance Program (APIP) have this cyber liability insurance coverage. Check with your agency risk management office or with ORM to confirm if your agency has this coverage.


6. What are the policy limits?

The state has a limit of \$1,000,000 per claim per agency subject to a \$5,000,000 annual aggregate (the maximum that the insurance company will pay in any policy period) in the current policy year for most coverages.

7. Does the Self Insurance Liability Program (SILP) provide cyber liability coverage?

Yes, however, SILP will only pay in the event the state receives a valid claim for tort damages resulting from breach by the state of a duty owed to the third party. Here is an illustration of how the various liability insurance policies would work in this case:

Cumulative Limits	1st Party Damage	3rd Party Liability
\$11M		Primary SILP (\$10M)
\$1M	Small Agency Cyber Liability Insurance (\$1M)	
	Agency Pays \$250,000.00	





8. Is this expensive insurance?

No. Agencies in this program do not pay a premium. In 2023, the State Legislature provided funding to purchase cyber liability coverage for small agencies when APIP is not a cost-effective option.

9. When should agencies report to ORM that they may have a data breach?

Short answer: As soon as possible. No incident is too small or too big to report.

During a privacy or security incident that has the potential to be a data breach, time is of the essence. [RCW 42.56.590](#) requires notice be given to affected residents of the state within 45 days. Notice to residences outside of Washington could have shorter timelines.

Agencies should not hesitate to contact the ORM as well as your Assistant Attorney General (AAG), and if you suspect a security related cyber incident, contact the Office of Cyber Security (OCS). Getting this team together early will provide agency management with the best information to help them make difficult decisions and take appropriate timely actions.

Our cyber liability insurance policies provide access to mature vendors who are in the incident response business. We have access to national level firms for specialized legal assistance, forensic investigation assistance, production of notices and mailing, call center operations, and credit monitoring services. When you tell us you have an incident, we act as a facilitator to get appropriate resources deployed to support you.

10. How do we find out more about this policy or report a claim or incident?

ORM contacts are Tiffany Gowon, 360-701-3487, tiffany.gowon@des.wa.gov or Kim Haggard, 360-407-8139, kimberly.haggard@des.wa.gov.

11. Can an agency get more cyber liability Insurance?

Yes, contact ORM and request a quote. We will work with you and the state insurance broker to find a policy that meets your needs.



INDIVIDUAL AGENCY COVERAGE SUMMARY

Cyber, Privacy and Network Security Liability:

LIMIT: \$1,000,000 per claim/\$5,000,000 annual aggregate for all coverages

A claim (e.g., someone files a tort claim against the state) for damages and claims' expense, in excess of the deductible, which the state of Washington becomes legally obligated to pay because of a:

- Theft, loss, or unauthorized disclosure of personally identifiable, non-public information or third party corporate information in the care, custody or control of the state of Washington or an independent contractor that is holding, processing or transferring such information on behalf of the state of Washington.
- Failure of computer security to prevent a security breach including:
 - Alteration, corruption, destruction, deletion, or damage to a data asset stored on computer systems.
 - Failure to prevent transmission of malicious code from state of Washington computer systems to third party computer systems.
 - Participation by state of Washington computer systems in a denial of service attack directed against a third party computer system.
- Failure to disclose any of the above incidents in a timely manner in violation of any breach notice law.
- Failure to comply with state of Washington privacy law or agency privacy policy.
- Failure to administer an identity theft prevention program or take necessary actions to prevent identity theft required by governmental statute or regulation.

Cyber Incident Response Team:

LIMIT: \$1,000,000 per claim/\$5,000,000 annual aggregate for all coverages

Privacy notification costs, in excess of the deductible and incurred by the state of Washington with underwriters' prior consent resulting from a legal obligation to comply with breach notice law because of an incident or reasonably suspected incident.



NOTE: Privacy notification costs shall not include any internal salary or overhead expense of the state of Washington.

Regulatory Proceedings:

LIMIT: \$1,000,000 per claim/\$5,000,000 annual aggregate for all coverages

Claims expenses and penalties the state of Washington is legally obligated to pay, in excess of the retention amount (deductible), from a regulatory proceeding resulting from a violation of a privacy law caused by an incident or reasonably suspected incident.

Payment Card Loss:

LIMIT: \$1,000,000 per claim/\$5,000,000 annual aggregate for all coverages

Payment Card Loss (e.g. credit cards, debit cards) means monetary assessments, fines, penalties, chargebacks, reimbursements, and fraud recoveries, including card reissuance costs, which an Insured becomes legally obligated to pay as a result of an Insured's actual or alleged failure of network security or the improper management of a card.

Electronic, Social and Printed Media Liability:

LIMIT: \$1,000,000 per claim/\$5,000,000 annual aggregate for all coverages

A claim (e.g., someone files a tort claim against the state) for damages and claims expense, in excess of the deductible, for which the state of Washington becomes legally obligated to pay resulting from any one or more of the following acts:

- Defamation, libel, slander, trade libel, infliction of emotional distress, outrage, outrageous conduct, or other tort related disparagement or harm to the reputation or character of any person or organization.
- A violation of the rights of privacy of an individual, including false light and public disclosure of private facts.
- Invasion or interference with an individual's right of privacy, including commercial appropriation of name, persona, voice or likeness.
- Plagiarism, piracy, misappropriation of ideas under implied contracts.
- Infringement of copyright.



- Infringement of domain name, trademark, trade name, trade dress, logo, title, metatag, slogan, service mark, or service name.
- Improper deep-linking or framing within electronic content.

Network Extortion Threat/Ransomware:

LIMIT: \$1,000,000 per claim/\$5,000,000 annual aggregate for all coverages

Network extortion loss, in excess of the retention amount (deductible), incurred by the state of Washington as a direct result of an extortion threat by a person, other than the state's employees, directors, officers, principals, trustees, governors, managers, members, management committee, members of the management board, partners, contractors, outsourcers, or any person in collusion with any of the foregoing.

*Ransomware only available to agencies with full MFA in place for remote and email access to State systems. Check with your agency's Risk Manager to verify your status.

Digital Data Recovery:

LIMIT: \$1,000,000 per claim/\$5,000,000 annual aggregate for all coverages

Data protection loss, in excess of the retention amount (deductible), for data loss by the state of Washington as a direct result of alteration, corruption, destruction, deletion or damage to a data asset, or the inability to access a data asset that is a direct result of a failure of computer security to prevent a security breach.

Business Interruption Loss and Extra Expenses:

LIMIT: \$1,000,000 per claim/\$5,000,000 annual aggregate for all coverages

Business interruption loss, in excess of the retention amount (deductible), for income loss and extra expenses during a period of restoration following a network interruption that is directly caused by a failure of computer security to prevent a security breach.

Contingent Business Interruption Loss and Extra Expenses:

LIMIT: \$250,000 per claim/\$5,000,000 annual aggregate for all coverages.



Washington State
**DEPARTMENT OF
ENTERPRISE SERVICES**

Social Engineering:

LIMIT: \$250,000 per claim/\$5,000,000 annual aggregate for all coverages



DEFINITIONS

Breach Notice Law means any state, federal or foreign statute or regulation that requires notice to persons whose personally identifiable, non-public information was accessed or reasonably may have been accessed by an unauthorized person.

Claims Made means that this policy will pay out when an incident first takes place on or after the retroactive date (10/1/2014); and before the end of the policy period; and is discovered by the state of Washington and reported to Beazley. The retroactive date will most likely be constant for all future years this policy is in force.

Computer Systems means computers and associated input and output devices, data storage devices, networking equipment, and back up facilities operated by and either owned by or leased to the state of Washington; or systems operated by a third party service provider and used for the purpose of providing hosted computer application services to the state of Washington or for processing, maintaining, hosting or storing the state of Washington's electronic data, pursuant to written contract with the state of Washington for such services.

Data Asset means any software or electronic data that exists in computer systems and that is subject to regular back up procedures, including computer programs, applications, account information, customer information, private or personal information, marketing information, financial information and any other information necessary for use in the state of Washington's ordinary course of business.

Extortion Threat means a threat to breach computer security unless an extortion payment is received. The extortion threat may seek to:

- Alter, destroy, damage, delete or corrupt any data asset.
- Prevent access to computer systems or a data asset, including denial of service attack or encrypting a data asset and withholding the decryption key for such data asset.
- Perpetrate a theft or misuse of a data asset on computer systems through external access.
- Introduce malicious code into computer systems or to third party computers and systems from state computer systems.
- Interrupt or suspend computer systems.



Incident means an act or reasonably suspected act that results in a:

- Theft, loss, or unauthorized disclosure of personally identifiable, non-public information or third party corporate information in the care, custody or control of the state of Washington or an independent contractor that is holding, processing or transferring such information on behalf of the state of Washington.
- Failure of computer security to prevent a security breach including:
 - Alteration, corruption, destruction, deletion, or damage to a data asset stored on computer systems.
 - Failure to prevent transmission of malicious code from state of Washington computer systems to third party computer systems.
 - Participation by state of Washington computer systems in a denial of service attack directed against a third party computer system.
- Failure to timely disclose any of the above incidents in violation of any breach notice law.
- Failure to comply with state of Washington privacy law or agency privacy policy.
- Failure to administer an identity theft prevention program or take necessary actions to prevent identity theft required by governmental statute or regulation.

Malicious Code means any virus, Trojan horse, worm or any other similar software program, code or script intentionally designed to insert itself into computer memory or onto a computer disk and spread itself from one computer to another.

Privacy Notification means the following reasonable and necessary costs incurred by the state of Washington within one year of the reporting of the incident or suspected incident to the underwriters.

- To hire computer security experts to determine the existence and cause of any security breach and the extent to which non-public information was accessed.
- Fees charged by an attorney to determine the applicability of and actions necessary to comply with breach notice laws.
- Provide notification to individuals who are required to be notified by the state of Washington in applicable breach notice law.



- At the underwriters discretion, to individuals affected by an incident in which their personally identifiable, non-public information has been subject to theft, loss, or unauthorized disclosures in a manner which compromises the security or privacy of such individual by posing a significant risk of financial, reputational or other harm to the individual.
- Provide up to \$50,000 for the costs of a public relations consultancy for the purpose of averting or mitigating material damage to the state of Washington's reputation.
- Provide, at the underwriter's discretion, one year of credit monitoring services to those individuals whose personally identifiable, non-public information was compromised. Also, mailing and other reasonable third party administrative costs associated with credit monitoring services.

Social Engineering means the intentional misleading of a Covered Person by means of a dishonest statement or misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and which was relied upon by the Covered Person believing it to be genuine.