

Cyber Liability Insurance Overview

Policy Year 2021-2022

For policy year 2021-22, the Department of Enterprise Services, Office of Risk Management (ORM) has purchased cyber liability insurance from Alliant Insurance Services. Like last year, this insurance is available only to agencies who participate in the Alliant Property Insurance Program (APIP). Agencies in the APIP program have the following cyber liability insurance available:

APIP Cyber Liability Insurance – This policy provides the state with limits of \$2,000,000 per claim / \$2,000,000 aggregate subject to sub-limits where applicable. This policy has changed (explained below) relative to the 2020-21 term.

Important Note: The APIP program is a public entity insurance solution with over 8,000 members with a total insurable value of \$400 Billion. The state of Washington is one of the 8,000 members of this program. The APIP cyber liability insurance has a \$40,000,000 aggregate limit for the entire APIP program for the 2021-22 year. This means that in the event other APIP program members have significant cyber liability claims, the limit could be exceeded and result in no available insurance for Washington. This represents a risk to the state.

Excess Cyber Liability Insurance – We have added an excess cyber liability insurance policy that sits above the primary APIP cyber liability insurance policy. The excess policy does several important things for the state: It is not shared with anyone – it is only for Washington State:

- It adds \$3,000,000 to our APIP cyber liability insurance limits.
- It provides exactly the same coverages that are in the APIP cyber liability insurance, subject to sub-limits where applicable.
- It also has a “drop down” provision which would apply when the APIP cyber liability insurance is not be available because of exhaustion of the APIP pool \$40,000,000 aggregate limits or our own \$2,000,000 limit. Even if the APIP primary insurance limits are gone, we still have available at least up to \$3,000,000 in cyber liability insurance, subject to sub-limits where applicable.

Together, these two insurance policies provide the state a combined maximum cyber liability insurance limit of \$5,000,000 per claim / \$5,000,000 aggregate, subject to sub-limits where applicable. This document provides an overview of the cyber liability insurance policies, 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.

	Primary	Excess Layer	Combined
Insurance Company	APIP Beazley	Indian Harbor Insurance Co	
A.M. Best Rating	A (Excellent) XII (\$1B to \$1.25B)	A (Excellent) XV (\$2B+)	
Coverage Form	Primary Cyber Liability	Excess Liability Follow Form	
Policy Limits	\$2,000,000	\$3,000,000	\$5,000,000
Privacy Notification Limits			
Beazley Approved Vendors	\$1,000,000	\$1,000,000	\$2,000,000
Non Beazley Approved Vendors	\$500,000	\$500,000	\$1,000,000
Business Interruption resulting from a security breach	\$750,000	\$750,000	\$1,500,000
Cyber Extortion Loss	\$750,000	\$750,000	\$1,500,000
Data Recovery Loss	\$750,000	\$750,000	\$1,500,000
Computer Hardware (Bricking)	\$100,000	\$100,000	\$200,000
Aggregate Limits			
APIP Program	\$40,000,000		
State of WA	\$2,000,000	\$3,000,000	\$5,000,000
Deductible	\$250,000	NA	\$250,000

Policy period: 07/01/2021 - 06/30/2022

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

Retroactive Date: Primary (APIP) 10/01/2014
Excess (XL) 07/01/2017

Policy Number: Primary (APIP) FN2105500
Excess (XL) **TBD**

Frequently Asked Questions

The following responses to common questions reflect the high points of our current 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 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 third-party would be 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 \$100,000 as a deductible and the cyber liability insurance would pay the remaining \$500,000.

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 combined cyber liability insurance policies?

The self-insurance deductible amount is \$250,000.

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.

- Beazley Syndicate of Lloyds of London provides our current cyber liability insurance. Beazley is AM Best rated A (excellent, stable and strong), VIII. They are located in London however are licensed to do business in all 50 states and are specialists in property, cyber liability and professional indemnity insurance.
- Montana had a data breach of 1.3 million medical records in 2013. They have the same policy. The Montana State Risk Manager reported that they had an excellent experience from Beazley response resources.
- The cyber liability insurance policy is NOT based on any assessment of compliance to the state Office of the Chief Information Officer (OCIO) or other IT security standards at the time of a loss.
- During the 2015-2016 policy year, we had one significant claim against this policy related to the Health Care Authority (HCA) data breach. The policy and breach response vendors performed as expected. ○ The HCA Risk Manager said this to the insurance company: *“I want to take a moment to thank you for the quick turnaround and level of service we have received (including service from the vendors we are using to handle Notices and Credit Monitoring). Everyone involved has made an otherwise difficult situation much more bearable.”*
- The state CIO asked the HCA CIO if this insurance and the resources it provides was helpful, his reply: *“Easy answers. Yes, we used them and the experience, to quote our risk manager, has been phenomenal. They have been responsive, helpful, and just made this whole process easier for us.”*
- During the 2016-2017 policy year, we had two significant incidents and the policy performed as expected.

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

No, only agencies that participate in the Alliant Property Insurance Program 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 \$5,000,000 per claim and 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. Please refer to the table on page 2 for noteworthy sub-limits. It is necessary to notify the insurer immediately of a potential incident in order to maximize available coverage.

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	1 st Party Damage	3 rd Party Liability
\$15M		Primary SILP (\$10M)
\$5M	Excess Cyber Liability Insurance (\$3M)	
\$2M	Primary APIP Cyber Liability Insurance (\$2M)	
	Agency Pays \$250,000 Retention	

Note: SILP provides \$10 Million in tort liability insurance coverage for most agencies. DSHS, DOC, and DOT have different amounts of SILP coverage. When combined, APIP Cyber, Primary SILP and total \$15 Million in tort liability insurance coverage for all agencies, provided aggregate limits remain under the APIP Cyber policy.

8. Why did the state purchase the Cyber Liability Excess Policy?

As outlined above, the APIP cyber liability insurance policy has a significant risk - the insurance may not be available when needed. During 2015, we surveyed many state agency risk managers who indicated they were concerned about this risk. The ORM worked with our insurance broker to build an excess insurance policy that addressed this risk and is affordable.

9. Is this expensive insurance?

No. Agencies in the APIP program will pay \$2,535.60 or \$7,755.36 per year for up to \$5,000,000 of insurance coverage. Agencies in this program who have a higher level of cyber risk will pay more than those who have a lower level of cyber risk.

10. 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.

For agencies not in the APIP, we have master contracts in place for breach response services with the same vendors the insurance company provides.

11. How has this insurance performed for the recent data breach events involving Washington State Agencies?

We have had an excellent experience so far. We have had three significant data breach events, one in the 2015-2016 policy year and two in the 2016-2017 policy year. We filed these incidents with Beazley and they provided resources and covered costs as expected. The Attorney General's Office (AGO) has processes in place to quickly implement the required Special Assistant Attorney General (SAAG) agreements for outside legal experts. During the most recent event, this agreement was operational in one business day. Getting a legal expert to work closely with your agency leadership and assigned AAG's is the most important incident response step to do quickly.

More recently, the State has experienced losses in different areas, including incidents arising out of vendors of ours having been impacted by ransomware type attacks. Another example of a more recent loss that is ongoing had to do with the suspected introduction of malware into a state computer system. Both of these incidents resulted in costly efforts to respond, and the claims are ongoing.

12. Have there been challenges using this insurance in the three cases mentioned above?

Yes. There have been challenges with state incident response processes. Beazley has been easy to work with. We still have room for improving our data breach incident response planning. Every agency should develop a plan to respond to a major data breach event and practice it.

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

ORM contacts are Tiffany Bradley, 360-701-3487; Kim Haggard, 360-280-6962, kimberly.haggard@des.wa.gov or Jason Siems, 360-407-8729, jason.siems@des.wa.gov.

14. 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.

15. My agency is not currently part of the APIP program. Can we join the APIP program during the policy year and obtain the cyber liability insurance offered through APIP or do we need to wait for the next policy period?

An agency could join APIP at any time during a policy year. They would be required to insure a reasonable amount of property. Call the ORM contacts listed previously for assistance.

Coverage Summary

Information Security & Privacy Liability Coverage (A):

LIMIT: \$5,000,000 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.

Privacy Notification Costs Coverage (B)

LIMIT: \$2,000,000 per claim/\$2,000,000 annual aggregate for all coverages (provided Beazley resources are used, otherwise \$1,000,000 per claim/\$1,000,000 annual aggregate)

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 Defense and Penalties Coverage (C)

LIMIT: \$5,000,000 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.

Website Media Content Liability Coverage (D)

LIMIT: \$5,000,000 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.

Cyber Extortion Coverage (E)

LIMIT: \$1,500,000 per claim/\$1,500,000 annual aggregate for all coverages

Cyber 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.

First Party Data Protection Coverage (F)

LIMIT: \$1,500,000 per claim/\$1,500,000 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.

First Party Network Business Interruption Coverage (G)

LIMIT: \$1,500,000 per claim/\$1,500,000 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.

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, provision for mailing and other reasonable third party administrative costs associated with credit monitoring services.