Cyber Liability Insurance Overview

Policy Year 2016-2017

For policy year 2016-2017, the Department of Enterprise Services, Office of Risk Management has purchased cyber liability insurance from Alliant Insurance Services. Like last year, this insurance is available only to the 73 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 for most coverages. This policy has the same coverages (explained below) and sub-limits that were available in 2015-2016.

  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 $25,000,000 aggregate limit for the entire APIP program. This means that in the event other APIP program members have significant cyber liability claims, this limit could be exceeded. The result would be no insurance for Washington. That represents a risk to the state.

- **Excess Cyber Liability Insurance** – This year 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:
  - This policy is not shared with anyone – all ours
  - This policy adds $3,000,000 to our APIP cyber liability insurance limits.
  - This policy provides exactly the same coverages that are in the APIP cyber liability insurance.
  - This policy also has a "drop down" provision should the APIP cyber liability insurance not be available because of exhaustion of the APIP pool $25,000,000 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.

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 for all but one coverage. The exception is the notification coverage, which would have a combined $4,000,000 per claim / $4,000,000 aggregate limit.

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 the Office of Risk Management, contains additional descriptions, definitions, and exclusions.

Washington State Department of Enterprise Services

Policy Summary

	2015-2016	2016-2017		
		Primary Layer	Excess Layer	Combined
Insurance Company	APIP Beazley	APIP Beazley	XL Catlin Indian Harbor Ins Co.	
A.M. Best Rating	A (Excellent) XII ($1B to $1.25B)	A (Excellent) XII ($1B to $1.25B)	A (Excellent) XV ($2B+)	
Coverage Form	Primary Cyber Liability	Primary Cyber Liability	Excess Liability Follow Form	
Policy Limits	$2,000,000	$2,000,000	$3,000,000	**$5,000,000**
Privacy Notification Limits				
Beazley Approved Vendors	$1,000,000	$1,000,000	$3,000,000	**$4,000,000**
Non Beazley Approved Vendors	$500,000	$500,000	$3,000,000	**$3,500,000**
Aggregate Limits				
APIP Program	$25,000,000	$25,000,000		
State of Washington	$2,000,000	$2,000,000	$3,000,000	**$5,000,000**
Deductible	$100,000	$100,000	$100,000	**$100,000**

Policy period: 07/01/2016 - 06/30/2017

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) 07/01/2016

Policy Number:
Primary (APIP) PH 1533938
Excess (XL) MTE 9033705

Washington State Department of Enterprise Services

Frequently Asked Questions

The following responses to common questions reflect the high points of our current Cyber Liability Insurance policy. Please contact the Office of Risk Management 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 are the specific insurance coverages provided by this policy?**

   To understand how cyber liability insurance is structured, think about your home owner's insurance policy. You have 1st party damages insurance that covers things like fire and water damage, and you have 3rd party liability coverage in case your tree falls on your neighbor. Cyber liability insurance has 1st party damage coverage and 3rd party liability coverage. In this case the 1st party is the state of Washington and the 3rd party would be citizens whose information we have in our computer systems in the form of data.

   Let's say 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. The agency that experienced this incident would be required by that regulation to give notice to the 200,000 people. The cost to do that would be a 1st party damage. If the breach causes damage to the citizens and they file a tort claim against the state we could have a 3rd party liability. 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 retention (SIR) amount is $100,000. The terms SIR, retention, and deductible mean the same thing. The insurance covers costs over this limit.

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.

- Our current cyber liability Insurance is provided by the Beazley Syndicate of Lloyds of London. Beazley is AM Best rated A (excellent, stable and strong), VIII. This company is based in London but is licensed to do business in all 50 states. They are specialists in: property, cyber liability and professional indemnity.
- Montana had a data breach of 1.3 million medical records in 2013. They have this 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*."

5. Are all state agencies covered by the cyber liability insurance policy?

No, only agencies that participate in the Alliant Property Insurance Program have this cyber liability insurance coverage. Check with your agency risk management officer or with DES Office of Risk Management to see if your agency has this coverage.

6. What are the policy limits?

The state of Washington 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.

The exception is the Privacy Notification coverage. The primary APIP policy has sub-limits of $1,000,000 if we use breach response vendors approved by the APIP insurance company, only $500,000 if we don't. This coverage provides cost reimbursement for direct costs related to

forensic analysis, preparing and mailing notices, running a call center to answer citizen questions, and for one year of credit monitoring. Costs related to hiring public relations and legal experts are also covered to a maximum of $50,000 per claim.

The excess cyber liability policy adds $3,000,000 to this coverage. That means that we have a maximum of $4,000,000 for notification services if we use the approved vendors.

7. Isn't cyber liability coverage provided by the Self Insurance Liability Program (SILP)?

Yes, however, SILP will only pay in the event the state of Washington 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:

<table>
<tr><th>Limits</th><th>1st Party Damage</th><th>3rd Party Liability</th></tr>
<tr><td>$55M</td><td rowspan="2"></td><td>Excess SILP ($50M)</td></tr>
<tr><td>$15M</td><td>Primary SILP ($10M)</td></tr>
<tr><td>$5M</td><td colspan="2">Excess Cyber Liability Inaurance ($3M)</td></tr>
<tr><td>$2M</td><td colspan="2">Primary APIP Cyber Liability Insurance ($2M)</td></tr>
<tr><td></td><td colspan="2">Agency Pays $100,000 Retention</td></tr>
</table>

Note: The Primary SILP is the state's Self-Insurance Liability Program. This program provides $10 Million in tort liability insurance coverage for most agencies. DSHS, DOC, and DOT have different amounts of SILP coverage. Combined the Primary SILP and Excess SILP total $50 Million in tort liability insurance coverage for all agencies.

8. Why was a Cyber Liability Excess Policy purchased?

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 and learned they were concerned about this risk. The DES Office of Risk Management worked with our insurance broker to build an excess insurance policy that fixed this problem and was affordable.

9. Is this expensive insurance?

No. , Agencies in the APIP program will pay $576.96-1327.49 per year for up to $5,000,000 of insurance coverage. Agencies in this program with higher cyber risk pay more than those with lower cyber risk.

10. When should agencies report to the Office of Risk Management 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. Agencies should not hesitate to contact the Office of Risk Management as well as your AAG, and if you suspect a security related cyber incident, contact WaTech Security. 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 program we have master contracts in place for breach response services with the same vendors the insurance company provides.

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

Contact the Office of Risk Management by phone or email. Cyber liability contacts are:
Doug Selix, 360-407-8081 doug.selix@des.wa.gov
John Christenson, 360-407-9461 john.christenson@des.wa.gov
Kim Haggard, 360-407-8139 kimberly.haggard@des.wa.gov

12. Can an agency get more cyber liability Insurance?

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

13. 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?

Yes. 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 DES Office of Risk Management for assistance.


Washington State Department of
Enterprise Services

Washington State Department of Enterprise Services

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 retention amount (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: $4,000,000 per claim/$4,000,000 annual aggregate for all coverages (provided Beazley resources are used, otherwise $3,500,000 per claim/$3,500,000 annual aggregate)

Privacy notification costs, in excess of the retention amount (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 retention amount (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: $5,000,000 per claim/$5,000,000 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 forgoing.

First Party Data Protection Coverage (F)

LIMIT: $5,000,000 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.

First Party Network Business Interruption Coverage (G)

LIMIT: $5,000,000 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.

Washington State Department of Enterprise Services

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 servicers 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.