

# APIP - Cyber Liability Insurance Coverages, Limits, and FAQ

---

The state of Washington purchases property insurance from Alliant Insurance Services through the Alliant Property Insurance Program (APIP). APIP includes a limited cyber liability insurance policy. Thus, agencies participating in the APIP property program also have some cyber liability insurance.

This document provides an overview of the APIP cyber liability insurance policy explaining specific cyber liability coverages and limits. The actual policy contains additional descriptions, definitions, and exclusions.

## Policy Structure

<b>Policy period:</b>	10/1/2014 - 7/1/2015
<b>Policy type:</b>	Claims Made (e.g. covered incidents must occur and be reported within the policy period)
<b>Coverages:</b>	1) Financial loss recovery 2) Incident response services
<b>Retroactive Date:</b>	10/01/2014
<b>Underwriter:</b>	Beazley Syndicate of Lloyds of London.

## Cyber Liability Policy Limits & Retention

1. \$2,000,000 per claim, \$2,000,000 annual (policy year) state of Washington aggregate limit.
2. \$25,000,000 annual APIP program aggregate limit for all participants in the APIP program. This program includes over 300 local and state government organizations in addition to Washington state. There is a risk that at a point in time when we would want this insurance coverage it may not be available because of this limit.
3. \$100,000 retention (deductible).

### Information Security & Privacy Liability Coverage (A):

**LIMIT:** \$2,000,000 per claim/\$2,000,000 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 for 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:** \$1,000,000 per claim/\$2,000,000 annual aggregate for all coverages (provided Beazley resources are used, otherwise only \$500,000 per claim)

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:** \$2,000,000 per claim/\$2,000,000 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:** \$2,000,000 per claim/\$2,000,000 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, or slogan, service mark, or service name.
- Improper deep-linking or framing within electronic content.

### Cyber Extortion Coverage (E)

**LIMIT:** \$2,000,000 per claim/\$2,000,000 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, or 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:** \$2,000,000 per claim/\$2,000,000 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:** \$2,000,000 per claim/\$2,000,000 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.

## 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 mitigation material damage to the state of Washington 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.

## **Frequently Asked Questions Cyber Liability Insurance**

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. Does Washington State have cyber liability insurance?**

Yes, we have limited cyber liability insurance coverage that became effective Oct. 1, 2014. This policy is to help cover costs associated with the financial impact from information technology (IT) security incidents.

- This coverage is provided as a feature of the property insurance policy the state carries. For an agency to access this coverage, it must have property insured under the Master Property Insurance Program. Our Master Property Insurance is provided by the “Alliant Property Insurance Program” (APIP). The underlying insurance is provided by the Beazley Syndicate of Lloyds of London. There are 320 large public governmental organizations in this program, including states, counties, and cities. The program has more than \$250 billion of insured property value.
- Authority to purchase insurance for the state can be found in RCW 43.19.760 – 781.

### **3. What are the specific cyber liability coverages?**

Please reference the Cyber Liability Insurance Coverages and Limits Document.

### **4. What is the deductible for the current cyber liability insurance policy?**

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.

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

The state requires our insurance broker to only offer us insurance 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.
- State of 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.

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

No, only agencies that participate in the Master Property Insurance Program have the current cyber liability insurance coverage. Check with your agency risk management officer to see if your agency has this coverage.

**7. What are the policy limits?**

In general the State of Washington has a limit of \$2,000,000 per claim and a \$2,000,000 annual aggregate (the maximum that the insurance company will pay in any policy period) in the current policy year.

The Public Entity Property Insurance Program has an aggregate limit of \$25,000,000 in the current policy year for all participants in the program.

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

Yes, only in the event that the State of Washington is sued for damages because of a cyber incident. The plaintiff in such litigation would have to prove harm from the cyber incident.

**9. What should agencies that are included in the policy report to the Office of Risk Management?**

This policy requires that the state provide notice of claim, loss, or circumstance that might lead to a claim as soon as practicable.

Keep the Office of Risk Management up to date regarding your agency cyber liability risk exposure.

**10. 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](mailto:doug.selix@des.wa.gov)  
John Christenson, 360-407-9461 [john.christenson@des.wa.gov](mailto:john.christenson@des.wa.gov)  
Kim Haggard, 360-407-8139 [kim.haggard@des.wa.gov](mailto:kim.haggard@des.wa.gov)

**11. Is this different than the OCIO Incident Communication Policy?**

Yes, the OCIO Incident Communication Policy deals with the operational communication needs during an IT Security incident. Cyber liability insurance and associated incident and claims reporting happens a little later when we are dealing with the impact from the incident. Agency IT leadership should work closely with their risk manager to develop procedures for these reporting requirements. Our obligation is to report claims and incidents as soon as practicable.

**12. How would an agency get more cyber liability Insurance than provided by this policy?**

Contact the Office of Risk Management and request a quote from our broker.