Cyber Liability Program
Coverage Summary

Insurance Policy Information:

Insurance Company	Beazley & Various
A.M. Best Rating	Varies
Standard & Poor's Rating	Varies
State Covered Status	Non-Admitted
Policy/Coverage Term	July 1, 2025 – July 1, 2026
Policy #	Various

This is a "claims-made and reported" policy:

This policy provides coverage on a claims-made and reported basis; except as otherwise provided, coverage applies only to claims first made against the Insured/Member and reported to underwriters during the policy period. Claims expenses shall reduce the applicable limit of liability and are subject to the applicable retention.

How to Report a Claim:

IMMEDIATE NOTICE should be made to Beazley Breach Response of all potential claims and circumstances (assistance, and cooperation clause applies)
Claim notification under this policy is to:

Beazley Breach Response
bbr.claims@beazley.com
(866) 567-8570

Copy to:
Donna Peterson
Alliant Insurance Services
560 Mission Street, 6th Floor
(415) 403-1466
Toll Free Voice: (877) 725-7695 / Fax: (415) 403-1466
donna.peterson@alliant.com

Emergency or After-Hours Reporting:
Robert Frey
Senior Vice President, Claims Manager
(415) 403-1445 / rfrey@alliant.com

How to Request a Certificate of Insurance:

1. Request a Certificate of Insurance within the Members Only section of www.CSURMA.org … **OR**
2. Email an Alliant staff member directly:

La Shaunda Wallace (primary)
LaShaunda.Wallace@alliant.com
415-403-1489

Tevea Him (secondary)
thim@alliant.com
415-403-1416

This insurance document is furnished to you as a matter of information for your convenience. It only summarizes the listed policy(ies) and is not intended to reflect all the terms and conditions or exclusions of such policy(ies). Moreover, the information contained in this document reflects coverage as of the effective date(s) this document was created and does not include subsequent changes. This document is not an insurance policy and does not amend, alter, or extend the coverage afforded by the listed policy(ies) and the policy(ies) listed are subject to all the terms, exclusions, and conditions of such policy(ies).

Named Covered Entity:

1. California State University Risk Management Authority (CSURMA)
2. CSURMA Auxiliary Organizations Risk Management Alliance (AORMA)

Limits and Retentions: *(Limits are Aggregate for Each Member / Insured)*

Limits:

1.	Per Member Limit	$28,000,000
2.	Dedicated CSU Aggregate Limit	$43,000,000
3.	Notified Lives	2,000,000
4.	Legal/Forensics/PR/Crisis Management	$2,500,000
5.	Additional Breach Response Costs w/ Beazley Vendors	$28,000,000
6.	Business Interruption - System Failure	$28,000,000
7.	Dependent Business Interruption - Security Breach (IT Vendors Only in the excess)	$5,250,000
8.	Dependent Business Interruption - System Failure	$700,000
9.	Fraudulent Instruction	$525,000
10.	Telephone Fraud	$525,000
11.	Funds Transfer Fraud	$525,000
12.	Computer Hardware Replacement	$1,400,000
13.	Invoice Manipulation	$700,000
14.	Reputation Loss	$1,400,000
15.	Cryptojacking	$350,000
16.	Data Recovery	$28,000,000
17.	Cyber Extortion	$28,000,000
18.	Business Interruption - Security Failure	$28,000,000

Retentions:

1.	Per Claim for Member/Insured with Total Insured Values up to $250,000,000 at time of Policy Inception	$50,000
2.	Per Claim for Member/Insured with Total Insured Values greater than $250,000,000 and up to $750,000,000 at time of Policy Inception	$100,000
3.	Per Claim for Member/Insured with Total Insured Values greater than $750,000,000 at time of Policy Inception	$250,000
4.	CSU Auxiliary Organizations	$15,000
5.	Dependent/Business Interruption Loss	8 Hour Waiting Period

6. Breach Response Notified individuals 250

Specific Coverage Provisions / Definitions:

1. **Breach Response:** Indemnifies the Insured/Member for Breach Response Costs incurred by the Insured/Member because of an actual or reasonably suspected Data Breach or Security Breach that the Insured first discovers during the Policy Period

2. **First Party Loss:**

   a. **Business Interruption Loss** - Indemnifies the Insured/Member for a Business Interruption Loss sustained as a result of a Security Breach or System Failure that the Insured first discovers during the Policy Period

   b. **Dependent Business Interruption Loss** - Indemnifies the Insured/Member for a Dependent Business Interruption Loss sustained as a result of a Security Breach or a System Failure that the Insured first discovers during the Policy Period

   c. **Cyber Extortion Loss** - Indemnifies the Insured/Member for a Cyber Extortion Loss incurred as a result of an Extortion Threat first made against the Insured/Member during the Policy Period

   d. **Data Recovery Costs** - Indemnifies the Insured/Member for Data Recovery Costs incurred as a direct result of a Security Breach or System Failure that the Insured first discovers during the Policy Period

3. **Liability:**

   a. **Data & Network Liability** pays Damages and Claims Expenses, which the Insured is legally obligated to pay because of any Claim first made against any Insured during the Policy Period for a Data Breach, a Security Breach, the Insured's failure to disclose a Data Breach or Security Breach, or failure of the Insured to comply with the part of a Privacy Policy that specifically is related to disclosure, access or procedures related to Personally Identifiable Information.

   b. **Regulatory Defense & Penalties** pays Penalties and Claims Expenses, which the Insured is legally obligated to pay because of a Regulatory Proceeding first made against any Insured during the Policy Period for a Data Breach or a Security Breach.

   c. **Payment Card Liabilities & Costs** indemnifies the Insured/Member for PCI Fines, Expenses and Costs which it is legally obligated to pay because of a Claim first made against any Insured during the Policy Period.

   d. **Media Liability** pays Damages and Claims Expenses, which the Insured is legally obligated to pay because of any Claim first made against any Insured during the Policy Period for electronic Media Liability.

4. **e-Crime:** Indemnifies the Insured/Member for any direct financial loss sustained resulting from (a) fraudulent instruction, (b) funds transfer fraud, and (c) telephone fraud, that the Insured first discovers during the policy period.

5. **Criminal Reward**

   a. **Criminal Reward** - Indemnifies the Insured/Member for Criminal Reward Funds.

b. **Reputational Loss** - indemnifies the Insured Organization for Reputation Loss that the Insured Organization sustains solely as a result of an Adverse Media Event that occurs during the Policy Period, concerning: a Data Breach, Security Breach, or Extortion Threat that the Insured first discovers during the Policy Period

c. **Computer Hardware Replacement Costs** - is part of the Extra Expense coverage. Extra Expense means reasonable and necessary expenses incurred by the Insured Organization during the Period of Restoration to minimize, reduce or avoid Income Loss, over and above those expenses the Insured Organization would have incurred had no Security Breach, System Failure, Dependent Security Breach or Dependent System Failure occurred; and includes reasonable and necessary expenses incurred by the Insured Organization to replace computers or any associated devices or equipment operated by, and either owned by or leased to, the Insured Organization that are unable to function as intended due to corruption or destruction of software or firmware directly resulting from a Security Breach

d. **Invoice Manipulation** - indemnifies the Insured Organization for Direct Net Loss resulting directly from the Insured Organization's inability to collect Payment for any goods, products or services after such goods, products or services have been transferred to a third party, as a result of Invoice Manipulation that the Insured first discovers during the Policy Period. Invoice Manipulation means the release or distribution of any fraudulent invoice or fraudulent payment instruction to a third party as a direct result of a Security Breach or a Data Breach.

e. **Cryptojacking** - indemnifies the Insured Organization for any direct financial loss sustained resulting from Cryptojacking that the Insured first discovers during the Policy Period. Cryptojacking means the Unauthorized Access or Use of Computer Systems to mine for Digital Currency that directly results in additional costs incurred by the Insured Organization for electricity, natural gas, oil, or internet.

Exclusions: *(including but not limited to)*

1. Bodily Injury or Property Damage
2. Trade Practices and Antitrust
3. Prior Known Acts & Prior Noticed Claims
4. Sale or Ownership of Securities & Violation of Securities Laws
5. Criminal, Intentional of Fraudulent Acts
6. Patent, Software Copyright, Misappropriation of Information
7. Governmental Actions
8. Other Insureds & Related Enterprises
9. Media-Related Exposures – Contractual liability or obligation
10. War and Cyber War Exclusion with Single Entity Carve Back
11. First Party Loss – with respects: 1. seizure, nationalization, confiscation, or destruction of property or data by order of any governmental or public authority; 2. costs or expenses incurred by the Insured to identify or remediate software program errors or vulnerabilities or update,

replace, restore, assemble, reproduce, recollect or enhance data or Computer Systems to a level beyond that which existed prior to a Security Breach, System Failure, Dependent Security Breach, Dependent System Failure or Extortion Threat; 3. failure or malfunction of satellites or of power, utility, mechanical or telecommunications (including internet) infrastructure or services that are not under the Insured Organization's direct operational control; or 4. fire, flood, earthquake, volcanic eruption, explosion, lightning, wind, hail, tidal wave, landslide, act of God or other physical event.

Questions:

Thomas Joyce	Mimi Long	Van Rin
415-403-1417	415-403-1423	415-403-1408
thomas.joyce@alliant.com	mlong@alliant.com	vrin@alliant.com