Due Diligence Information

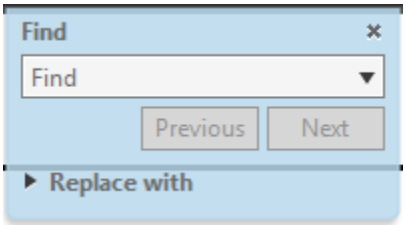
Corporate Basic Package

CUNA Mutual Group makes this package available to you to fulfill your organization's due diligence obligations involving third party relationships.

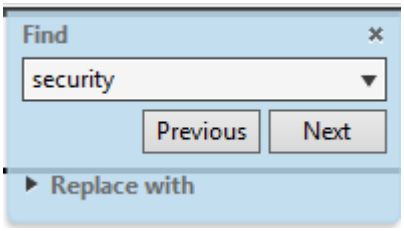
In providing this information, we want to remind you that the information is confidential and proprietary to CUNA Mutual Group. Product or program specific due diligence information may also be attached.

To search this document:

1. Select **Edit** from the menu bar
2. Click **Find** and the **Find** box will display



3. Enter your '**topic'** of interest in the Find field



4. Click **Next, t**he **Find** function will highlight the matches in blue.
5. Navigate through the matches with the **Previous** and **Next** buttons

We trust the attached information will satisfy the fulfillment of your due diligence obligations. If you have any questions, please contact us.

© 2021 CUNA Mutual Group, All Rights Reserved.

Financial Information

(Annual Report, Financial Statements, Ratings)

CUNA Mutual Group's financial reports and ratings provide information on the company's financial results and business model. The following information is available in the **Financial Information** section within About Us on CUNA Mutual Group's website: www.cunamutual.com

About Us/Financial Information *(click on this link to access the following)*

- Current version of the Annual Report
- Current versions of the Consolidated Financial Statements and Independent Auditor's Report
- Financial ratings for certain entities of CUNA Mutual Group

Frequently Asked Questions

Question	Response
Please provide the most recent Audited Financial Statement with the Opinion for the organization.	The Financial Information page referenced above includes links to the current Consolidated Financial Statements and Independent Auditor's Report.
Has CUNA Mutual Group had any recent financial audit deficiencies?	Please reference the current Annual Report and/or the Consolidated Financial Statements and Independent Auditor's Report available on the Financial Information page referenced above.
Does your company have the financial ability to deliver the services and/or goods under the contract? Please provide a copy of the most recent available audited financial statements to identify liquidity, outstanding capital commitments, capital strengths, and operating results.	The Financial Information page referenced above includes links to the Consolidated Financial Statements and Independent Auditor's Report.
Can you provide A.M. Best Ratings?	The Financial Information page referenced above includes A.M. Best Company's ratings and additional rating agency ratings.

© 2021 CUNA Mutual Group, All Rights Reserved.

Privacy Policy

CUNA Mutual Group's Privacy Policy will help you understand how we collect, use, share and protect personal information we have about you. This Policy applies to CMFG Life Insurance Company, MEMBERS Life Insurance Company, CUNA Brokerage Services, Inc., CUMIS Insurance Society, Inc., and TruStage Insurance Agency, LLC. The information is available in the **Privacy Policy** section within About Us on CUNA Mutual Group's website: www.cunamutual.com.

About Us/Privacy Policy (click on this link to access the following):

- When this Policy applies
- Types of personal information we collect, where we get it, and why
- Who we share your personal information with, and why
- How your personal information is secured
- And more

© 2021 CUNA Mutual Group, All Rights Reserved.

Security Practices

CUNA Mutual Group takes our Information Security risk posture very seriously. This document is meant to give an overview of the practices that we follow to protect both our computer systems and the data that has been entrusted to us.

Policies and Procedures
Management has established security policies which are reviewed annually and communicated to all employees. The following general concepts are covered:

- Our security governance framework aligns security strategy with both business objectives and applicable laws and regulations.
- Management will fulfill its responsibilities by designing and implementing business practices based upon industry standards and best practices to protect against unauthorized access, use, disclosure or destruction of corporate information and technology.
- CUNA Mutual Group's position regarding the protection of customer information is derived from several corporate policies that have a bearing on the collection, use and protection of customer data.
- The policies ensure protection of assets not only through documented responsibilities, but also communicated expectations.
- All employees and contractors working on CUNA Mutual Group's behalf are responsible for conducting day-to-day accountabilities in a manner that is consistent with this policy.
- Corporate information and business applications are protected applying administrative, physical and technical safeguards.

Access Control
Access to CUNA Mutual Group's online services and business functions is secured by a unique user ID and password. Passwords must be changed regularly and must adhere to compliance with security policy. Password complexity is set up in order to decrease the risk of unauthorized access to data and business applications. A limited number of administrators have the authority to maintain these policies and setup new user accounts.

CUNA Mutual Group utilizes multi-factor authentication for remote access to our internal networks and for administrative access to our cloud infrastructure. Multi-factor authentication is also available on select CUNA Mutual Group digital properties.

Physical and Environmental Security
All computer hardware and storage media is stored in a limited access facility. Additionally, a copy of all production data and systems resides in a separate, secured facility. These facilities are secured 24-hours per day, 365 days a year, and monitored accordingly. A multi-factor key card system is in place to gain access to the building as well as access to the computer facilities. The key card system logs all activity from the card readers. The system records the card number swiped, date and time and action performed. These logs are reviewed periodically by Computer Operations management. Access to the computer facilities is limited based on an individual's job responsibilities.

The computer facilities are environmentally controlled. Power is protected by a generator with two independent power feeds. If the generator itself fails, two UPS units provide power to allow for controlled shutdown of equipment. The generator and UPS units are configured to provide as much redundancy in power delivery routes as possible. A separate fire system using dry sprinklers is installed.

Data Encryption
CUNA Mutual Group utilizes data encryption for our online business services that require data transmission. Internally, we have multiple methods to encrypt, mask or tokenize data while in transit and at rest.

© 2021 CUNA Mutual Group, All Rights Reserved.

Anti-Virus/Malware
CUNA Mutual Group utilizes End Point Protection capabilities to scan for viruses and other malicious software. Antivirus software is deployed on our mail service and servers, as well as on all desktops and laptops. Virus "signature" files are updated as signatures become available. In addition, emergency procedures designed to contain malware outbreaks are in place.

Data Loss Prevention
CUNA Mutual Group utilizes Data Loss Prevention capabilities to ensure sensitive data does not leave the corporate network.

Intrusion Detection Capabilities and Firewalls
Intrusion Detection and Prevention systems are in place through which we monitor internal network traffic as well as network traffic to and from the Internet. These systems are designed to detect and block suspicious network traffic. In addition, our segmented networks are also protected by firewalls, proxies, DNS controls and other network security devices and services which further serve to detect, filter and block potentially malicious traffic.

Data Backup and Recovery Procedure
Our procedures require that all production data be backed up on a regularly scheduled basis. The data backup process is automated and monitored for any error situations. A large-scale recovery test is performed annually. Annual tests are conducted to ensure critical business processes can be recovered in a timely basis. Tests are also conducted to ensure that the recovery process is correct and that technology platforms and communications between them are operating as intended.

Independent Security Assessments
CUNA Mutual Group employs the services of various external consulting and auditing firms to validate our defenses and report on any findings discovered. In addition, CUNA Mutual Group obtains a statement of opinion regarding our penetration tests annually.

Incident Response
CUNA Mutual Group has established a formal process for evaluating and responding to security events and potential incidents. A core team from our cross functional areas are available in the event an incident involving our systems is detected. This team is charged with:

- Evaluating the incident
- Determining the appropriate mitigation strategy
- Determining the appropriate notifications to be made which may include law enforcement officials, customers and other third parties

Change Management
CUNA Mutual Group follows best practices for technology change management. The technology change management policy and process incorporate standardized methods and procedures for introducing changes into the production environment in a controlled manner to minimize any change-related service disruptions. The technology change management process utilizes industry best practices such as appropriate chain-of-approval prior to change implementation, oversight and monitoring of the change management process, and clear communications to stakeholders on upcoming changes.

Records Management
We have a formal Records Information Management Program, which is supported by a Records Retention Schedule, as well as departmental procedures. We also have procedures for storing, retrieving and destroying physical records. CUNA Mutual Group employs a total shredding program for all paper documents. Secured bins are provided for paper as well as electronic media for proper disposal.

Third Party Service Providers
CUNA Mutual Group assesses third party service providers' security controls and reviews their SSAE18 Audit Reports or equivalent to ensure they follow security best practices. The assessments are refreshed on a regular basis.

© 2021 CUNA Mutual Group, All Rights Reserved.

Pandemic Risk Plan
CUNA Mutual Group has a pandemic plan which covers the following risks: primary impact, business resiliency, pandemic, geographic concentration, remote work, and financial solvency. See our Pandemic Risk Frequently Asked Questions on the Due Diligence Center page on CUNA Mutual Group's website (www.cunamutual.com).

Frequently Asked Questions

Question	Response
Why is some security-related information not shared?	CMFG Life maintains a layered in-depth security defense. We take the security and confidentiality of our customer data very seriously. Some information may be proprietary and/or sensitive, while other information is not shared to help maintain the integrity and effectiveness of our information security posture. We consider it a best practice to maintain confidentiality regarding our data security practices, safeguards, and procedures. We believe that any other approach increases CUNA Mutual Group's vulnerability to attack.
Does CUNA Mutual Group maintain an internal control framework? Does it align with a particular industry standard?	Yes, we maintain a hybrid internal control framework derived from various sources such as PCI DSS, ISO 27001, NIST 800-53, ITIL, OWASP, CIS, COBIT and SSAE18. SOC 2 Service Principles and applicable regulations.
How does CUNA Mutual Group ensure its internal control framework remains effective?	Annually, we conduct various internal security risk assessments and engage multiple independent third parties to perform security assessments to ensure our internal security control framework remains effective. Reports and/or statements of opinion are available to our customers through our Due Diligence Center.
Does CUNA Mutual Group have a security/ incident response plan?	Yes, we have developed a comprehensive Security/Incident Response Plan which is reviewed on no less than an annual basis. (See "Incident Response" in the Security Practices section of the Basic Due Diligence Package.)
Do you provide or make available a formal security awareness training program for all persons with access to customer data?	Formal security awareness training is provided including annual mandatory training as are general awareness communications on various data privacy and security topics.
Does CUNA Mutual Group maintain a vulnerability and patch management process?	Yes, we actively scan our environment for vulnerabilities, assess vulnerability risks, and patch devices and applications as deemed appropriate.
Do you have anti-malware programs installed on all systems which support on premise and/or cloud service offerings?	Yes, we have anti-malware software installed on all managed devices and systems.
Are security information & event management related logs monitored and retained?	Yes, all pertinent logs are captured and monitored by a third-party service provider. Questionable log events are sent to our Incident Response Team for further analysis.
Are backups maintained off-site?	Yes, backups are maintained off-site.
Does CUNA Mutual Group follow a consistent change management process?	CUNA Mutual Group has a formal Change Management process utilizing industry best practices to ensure changes are implemented into the production environment in a controlled manner.

© 2021 CUNA Mutual Group, All Rights Reserved.

Question	Response
Does CUNA Mutual Group follow a consistent application development process?	CUNA Mutual Group follows a formal Software Development Lifecycle (SDLC) to ensure applications are developed in a consistent and secure manner across product lines.
What type of process or procedures does CUNA Mutual Group use to detect secure code defects in applications prior to production?	CUNA Mutual Group currently leverages static and dynamic code analysis, peer code reviews as well as vulnerability scans to detect secure code defects.
Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	Yes, CUNA Mutual Group has policies and procedures in place for de-provisioning of systems access.
Do you utilize encryption to protect data during transport across and between networks, as well as data at rest?	CUNA Mutual Group utilizes industry standard encryption methods to ensure confidentiality of sensitive information. We perform data encryption, masking or tokenization for data at rest and in transit and use least access privileges to restrict access to need to know.
Does your organization utilize Multi-Factor Authentication?	CUNA Mutual Group utilizes Multi-Factor Authentication for remote access to our internal networks and for administrative access to our cloud infrastructure. Multi-Factor Authentication is also available on select CUNA Mutual Group digital properties.
Do you have documented information security baselines for your infrastructure?	We maintain baseline hardening guides for our infrastructure components.
Do you ensure that security systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry best practices?	Yes, automated features are utilized to ensure security systems remain current or can be deployed real-time as warranted.
Do you have firewalls and network protection in place?	CUNA Mutual Group has multiple firewalls in place, as well as a number of network protection capabilities.
Are passwords required to be changed?	CUNA Mutual Group maintains a robust password policy for all identities.
Does CUNA Mutual Group have physical security controls for the datacenter?	Yes, we utilize a host of multi-layered security controls to protect the CUNA Mutual Group datacenter.
Are mechanisms in place to detect the presence of unauthorized network devices?	Yes, CUNA Mutual Group has implemented security mechanisms to continuously monitor its network for unauthorized devices.
Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes, CUNA Mutual Group has established procedures in place for approval, download and installation of software.

© 2021 CUNA Mutual Group, All Rights Reserved.

March 1, 2021
To whom it may concern:

As part of CMFG Life Insurance Company's ongoing commitment to ensuring the security and integrity of its systems and data, CMFG Life Insurance Company engaged NetSPI to perform a Internal Network Penetration Test; this testing was concluded on February 21, 2021. The purpose of this penetration test was to identify common security issues that could adversely affect the confidentiality, integrity, or availability of CMFG Life Insurance Company systems and data.

NetSPI security consultants follow a phased assessment approach for testing the security of enterprise networks. NetSPI consultants use multiple commercial and open-source security tools, custom scripts, and manual techniques to scan for, identify, and exploit vulnerabilities within the systems and devices tested. This methodology identifies an organization's tactical and strategic security challenges by taking a technical snapshot of the current state of security controls. NetSPI security consultants attempt to penetrate or circumvent existing security mechanisms by using software tools and exploit scripts that are like those used by attackers. In this manner, our approach analyzes the current security posture and results in recommendations for strengthening security controls.

Sincerely,
Charles Horton
COO

Sourcing & Vendor Management

This document is intended to outline CUNA Mutual Group's Sourcing and Vendor Management practices and controls. In addition to managing Vendor costs and performance, our controls have been designed to identify, review, and appropriately mitigate Vendor risks.

KEY TERMS

The following contains a list of key terms around CUNA Mutual Group's Sourcing and Vendor Management functions.

- **Enterprise Procurement Office (EPO)** is the department that oversees CUNA Mutual Group's Sourcing and Vendor Management functions and policies.
- **Vendor** is any unaffiliated third party that provides contracted products or services. This definition includes third-party administrators ("TPAs") and other relationships such as: Strategic Partnerships, Legal Services Providers, Third-Party Service Provides ("STPSP"), Joint Ventures, Broker Dealers, Insurance Agencies and Employee Benefits Providers.
- **Sourcing** is a process to evaluate and select one or more potential Vendors, resulting in a contract between a CUNA Mutual Group company and selected Vendor(s).
- **Stakeholders** are internal corporate functions that partner with the Enterprise Procurement Office in Vendor risk identification, risk monitoring and mitigation, cost control, and value optimization. Stakeholders include Legal, Information Security, Information Technology, Finance, Human Resources, etc.
- **Vendor Management** is a process and tools utilized to govern Vendor relationships, including: management of ongoing risks, realization of desired outcomes from Vendor partnerships, and management of contractual commitments.

PRACTICES AND CONTROLS

The following sections outline CUNA Mutual Group's key controls and practices on Sourcing and Vendor Management

A. Sourcing & Contracting

For every major Sourcing activity, EPO assigns a procurement lead to manage the following key activities:

- Identify and initiate the appropriate Sourcing process (e.g. RFx, Contracting, etc.).
- Completes an initial assessment which identifies any key risks related to the Sourcing and Contracting, including data sharing, system integrations, business continuity, etc.
- Engage the appropriate key Stakeholders based on the outcome of the initial assessment for ongoing involvement or consultation, which may include Legal, Information Security and other Stakeholders as needed.
- Manage Sourcing activities and work with Legal to manage Vendor negotiations to drive desired outcomes (e.g. advantageous pricing, favorable contract terms, and mitigation of identified risks).
- Work with Stakeholders to conduct any required due diligence of Vendor(s) such as reviewing financials and insurance, information security controls or other due diligence activities.

© 2020 CUNA Mutual Group, All Rights Reserved.

- Ensure contracts are reviewed and signed off by appropriate Stakeholders. Engagements in which an assumed risk exceeds enterprise risk tolerance standards may be escalated through a defined escalation path for further review and appropriate handling.

B. **Vendor Management**

For ongoing vendor management activities, EPO provides the following governance and support:

- Enterprise Procurement Office utilizes a ***Vendor Management Operational Risk Assessment ("VMORA")*** process that allows CUNA Mutual Group to appropriately tailor our Vendor Management practices and governance model to each Vendor's engagement.
- All Vendors are assigned a **Vendor Relationship Manager ("VRM")** who is accountable to manage the overall relationship with the vendor and serve as a single point of contact for EPO and Stakeholders on any vendor questions or requests.
- EPO builds a Vendor Management plan for the VRM based upon the VMORA. The plan will outline the required Vendor Management activities, as well as the frequency or date of each activity. Some required Vendor Management activities may include: business reviews, SLA reporting, financial due diligence, information security due diligence, review of certifications and insurance coverages, conducting site visits/audits, business resilience planning, disaster recovery testing, etc.
- EPO partners with the VRM to ensure required Vendor Management activities are performed, as well as to provide support and training.
- EPO and/or the VRM will also ensure appropriate Stakeholders are involved in any Vendor Management activities, if necessary.
- New tools and processes may be developed and utilized to effectively manage the Vendor, as necessary.

C. **Other Key Practices and Highlights**

In addition to optimizing costs, achieving favorable contracting terms**,** and mitigating risks, CUNA Mutual Group also values Vendor partnerships that enable socially responsible and sustainable practices.

- ***Supplier Diversity –*** CUNA Mutual Group involves Diversely-Owned Business Enterprises (DOBE) in Sourcing activities and gives fair and impartial consideration to products/services offered by a DOBE.
- ***Sustainability -*** CUNA Mutual Group evaluates Vendor partnerships and places emphasis on Vendors that provide environmentally friendly, sustainable products and services.

© 2020 CUNA Mutual Group, All Rights Reserved.

Standard Privacy/Security Terms For Third Party Service Providers

The following is an overview of the standard privacy and security contractual terms for our third party service providers ("TPSP") that host, store, process or have access to personal information relating to individual customers or prospective customers of the CUNA Mutual Group ("CUNA Mutual").

Confidentiality and Data Handling Requirements. We impose a number of basic non-disclosure and other confidentiality and security requirements intended to protect personal information and any other confidential or otherwise sensitive data that a TPSP might host, store, process or access in connection with our business/services relationship. These generally include:

- **CUNA Mutual Ownership of Data**. As between CUNA Mutual and the TPSP, CUNA Mutual owns all personal information and other data shared with the TPSP.
- **Confidentiality and Use of Data.** TPSP's must maintain the confidentiality of all personal information, and must not use or otherwise disclose any personal information except as required in connection with providing or performing services to or for CUNA Mutual.
- **Customer personal information stored in the U.S. only**.
- **Return/Destroy Upon Request or Termination**. TPSPs must return or destroy personal information and other data upon our request or upon termination of our agreement(s).

Compliance with Applicable Data Protection Laws. We require our TPSPs to comply with applicable data protection laws. This includes applicable privacy, data security and cybersecurity laws and regulations.

Notice of Security Incident. We require prompt notice in the event our TPSP becomes aware of or reasonably suspects any unauthorized access to or disclosure, acquisition, or use of personal information.

Information Security Program. We expect our TPSPs to implement and maintain an appropriate information security program that includes reasonable physical, technical and administrative measures to safeguard personal information, including but not limited to written information security policies and procedures, access controls, user identification and password standards, industry standard secure encryption methods to protect the data in transit or at rest, regular vulnerability scans, patch management processes, regular backups and secure logging of all access and changes to personal information.

Security Framework and Independent Security Assessment. We expect our TPSPs to conform to an appropriate security framework and, depending on the nature of the services provided, we may also require an annual or periodic independent 3rd party security audit (e.g., SOC 2 or other comparable audit).

Coding. For applicable TPSPs, we expect all software and computer code to be designed, developed or configured 1) using secure coding principles and methodologies generally accepted within the computer programming industry; 2) so as not to contain any known vulnerabilities or any embedded viruses, spy ware or other malware; and 3) in compliance with applicable and acceptable Open Source Software license terms and conditions, where applicable.

© 2021 CUNA Mutual Group, All Rights Reserved.

Business Resiliency Disclosure

I. Introduction

CUNA Mutual Group is committed to safeguarding business interests during an emergency or significant disruptive event. The company employs an enterprise business resiliency program designed to mitigate risk and provide continuity of operations.

Senior management actively supports the business resiliency program. Dedicated funding and staff are in place to enable actionable and comprehensive business resiliency planning and response.

This disclosure statement to our customers and business partners summarizes the Business Resiliency Program.

Due to proprietary information and privacy concerns the company does not publicly distribute specific program information.

II. Business Resiliency Program Policy

CUNA Mutual Group corporate policy requires critical business areas to maintain resiliency plans that ensure the enterprise's ability to provide continued insurance and financial products and services to our customers in compliance with applicable laws and regulations. The Business Resiliency Department is responsible for implementation and oversight of this program.

III. Business Resiliency Program Summary

The Business Resiliency Program provides framework, planning, training, exercises, and tools comprising a risk-based resiliency approach to ensure continuous operations should CUNA Mutual Group's employees, technology systems or business facilities be impacted by a disruptive event.

The program's methodology comprises three main components:

- Prepare
    - Impacts to time-sensitive business capabilities are routinely reviewed and are the basis for determining the recovery priority of these capabilities and associated products. This approach ensures that the recovery of business capabilities is appropriately prioritized to minimize customer impact.
    - Business resiliency plans reside in a secure hosted environment and are regularly exercised, either individually or collectively, using scenarios appropriate to the business functions, department staffs, and facilities. Plans address impacts to people, sites, resources, and technology systems. The program requires that all critical business areas review plans routinely and review if there are changes to business resiliency staffing or business capabilities.
    - CUNA Mutual Group maintains redundant systems and power sources, allowing critical data, telephone systems, and other key elements of our operational infrastructure to be maintained during a regional, local, or facility-related interruption.
- Respond
    - Crisis Response Teams are in place at all major CUNA Mutual Group locations. These cross-functional teams address the management of initial response and the strategies for recovery and continuation of operations. Team members are trained; their plans and duties are reviewed and exercised.
- Recover
    - Departments will continue to execute resiliency plans until all interrupted business services return to normal operations.

© 2021 CUNA Mutual Group, All Rights Reserved.

Frequently Asked Questions

Question	Response
Does CUNA Mutual Group have a disaster recovery plan?	Yes, see the Business Resiliency Program Policy and Summary described above.
Has a Business Impact Analysis been performed?	Yes, Business Impact Analyses for all business functions are regularly conducted. Proprietary information such as when the analyses are performed, and results cannot be provided.
Does CUNA Mutual Group have a pandemic plan?	Yes, see the Pandemic Risk Frequently Asked Questions on the Due Diligence Center page on CUNA Mutual Group's website (www.cunamutual.com).

© 2021 CUNA Mutual Group, All Rights Reserved.