Security Questionnaire – Attachment 10

External Vendor Information Security Questionnaire

Vendor Information			
Vendor Name	NathCorp Inc.		
Vendor Address	1 Park Plaza Suite 930, Irvine, CA 92614		
Vendor Contact(s)	**Name and Department**	**Email**	**Phone**
	Clark LaCombe	Clark.lacombe@nathcorp.com	323-828-3681
Date Completed or Updated	4/12/23		

Overview

Vendor has been identified as someone who does or will collect, use, exchange, store, view, access or destroy (collectively, "**Process**") the non-public information about Sun Life and its business, clients (including personally identifiable information about clients ("**Personal Information**")), employees, partners, information systems or other processes or procedures employed by Sun Life ("**Sun Life Information**").

Completion of the External Vendor Information Security Questionnaire is the first stage of the Information Security Risk Assessment process. The objective of the questionnaire is to provide Sun Life with an overview of the Vendor's environment and the security controls that have been implemented to protect Sun Life Information. In addition to the Information Security Questionnaire, the Sun Life Security Advisor may also interview key Vendor personnel that support the security function, review Vendor documentation and processes, review independent control assessments performed on Vendor, and perform an on-site security review.

This Information Security Questionnaire and your answers to these questions form part of your agreement with Sun Life.

Guidance on completing the questionnaire

The agreement between our organizations may be for multiple services, which can include Consulting /Professional Services, On Premise Software and Hardware, Hosting Services (SaaS, IaaS, and PaaS), Secure Storage or a combination of these services. We recommend that when completing the questionnaire, the responder view each question not only with a single product or service in mind, but also provide insight in to the overall organizational controls.

Where documents have been requested, please provide them separately and reference the document name in the response. If it is a large document supply the section and/or page # to direct us to the relevant information.

If there is a cloud environment, please indicate which responses relate to it.

A - General Company Information		
A1	List the geographic locations in which your company operates including data centres. a) Which locations will Sun Life Information be stored and/or processed? b) Are these locations owned and operated by your company?	NathCorp has locations in Ranchi India and Southern California. a) No Sun Life data will be stored in or processed in a NathCorp Data Center. b) All NathCorp data is stored in M365 and all work will be done in Sun Life Cloud Tenant or Data Center.
A2	Provide the following staffing numbers: a) Number of employees b) Number of IT Staff c) Number of Information Security staff d) Are the Information Security staff your employees, or a managed service provider?	a) 113 b) 10 c) 3 d) Employees

B - Overview of Systems and Applications that Handle or Store Sun Life Information				
B1	Describe the services that you provide to Sun Life (both current and intended).	System/application development for deliverables in scope as defined in the Sun Life IDP RFP.		
B2	Describe the services that you provide to Sun Life's clients (both current and intended).	N/A		
B3	List all of your systems/applications that do or will handle Sun Life Information (both current and intended). Provide an architecture diagram including data repositories and data flows of the systems	See architecture diagram supplied with the Sun Life IDP RFP.		
B5	Provide network topology diagram for the systems involved (including firewalls, servers, data centers, remote offices, etc.).	See architecture diagram supplied with the Sun Life IDP RFP.		
B6	Do you or will you have access to Sun Life's systems? If yes, provide the following details for each system to which you will have access: a) Name of Sun Life system you have access to b) For what business purpose c) How do you access the system? d) How do you get the approval and user privileges to access the system?	We have no current access. TBD - All requested access will be minimum required to satisfy deliverables in scope as defined in the Sun Life IDP RFP.		
B7	Describe how Sun Life information can be extracted from your applications and data repositories.	All NathCorp work will be done in Sun Life Cloud Tenant or Data Center.		
B8	Do you or will you be exchanging electronic data containing Sun Life Information with:	Sun Life	Sun Life clients	Third Parties
	a) What is the purpose of these exchanges?	N/A	N/A	N/A
	b) What type of information will be included in the exchange? Personally identifiable, health, and financial (PII, PHI, PFI) and other confidential information	N/A	N/A	N/A
	c) How is this done (e.g., email, FTP, web, API, etc.)?	N/A	N/A	N/A

B - Overview of Systems and Applications that Handle or Store Sun Life Information				
	d) Do you support encrypted transfer protocols (e.g., SFTP, VPN, HTTPS, Forced TLS, etc.)? i) If so what is the encryption algorithm and key strength? ii) If HTTPS is used, indicate protocols supported and whether older/insecure versions have been disabled (e.g., SSL v2/v3, TLS 1.1 or older).	Yes. i) We will always support the latest list of secure TLS Secure cipher suites. ii) All SSL will be disabled. TLS 1.1 and lower has been deprecated and will not be used.		Yes. i) We will always support the latest list of secure TLS Secure cipher suites. ii) All SSL will be disabled. TLS 1.1 and lower has been deprecated and will not be used.
	e) Is the data itself encrypted (e.g. files are encrypted with PGP, etc.)? If so, provide the encryption algorithm and key strength.	All data at rest will be encrypted. Our standard is AES-256		
	f) What volume of data (# of records) will be exchanged?	TBD. Pending Discovery and PoC.		
B9	Has there ever been a confirmed breach of your information systems (including unauthorized access to your information systems, exposure of client confidential data or intellectual property)?	No.		

C - Information Security Program		
C1	Describe the background check process on all candidates for employment, contractors, and third party personnel. Describe items being checked and for whom. (e.g., criminal records, credit history, identity, professional qualifications, work history, business references, etc.).	We use a third party to process background checks. The report includes past/current phone numbers, emails, addresses, relative's, associates, neighbors, criminal or traffic, bankruptcies, jobs and education, social media and assets.
C2	Do you have an Information Security Policy and supporting security standards that have been approved by management? a) Provide a copy of the Information Security Policy and any supporting security standards. If you cannot provide a full copy of the Security Policy or the supporting security standards, please provide: the Title Page, Table of Contents and Revision History.	Not at this time. But we are working on completing this. Our policy is to follow all customer policies and procedures while working for customers and handling customer data.

C - Information Security Program		
C3	Describe your Acceptable Use Policy for employees, contractors and third party personnel as it relates to handling information and using technology.	Computers must be kept up to date with OS and software patches, and used for work purposes only. NathCorp employees, contractors and third party personnel are responsible for following the customers Acceptable Use Policies.
C4	Describe your Information Classification standard and how your organization classifies information (i.e. based on its value, legal requirements, sensitivity, or criticality to the organization) and gives employees direction on how information in each classification is to be handled.	All NathCorp corporate data is sensitive and protected. We have 3 classifications, Confidential, Internal, and Restricted. Customer data is kept on the customer's site/tenant and must follow the customer's data handling and Acceptable Use Policies.
C5	Describe your Cryptographic standard and process to securely manage cryptographic keys. For cloud hosted solutions, do you manage the cryptographic processes for your environment? If not, then please describe the hosting provider's cryptographic key management procedures.	We have a Microsoft internal PKI infrastructure for internal use, GoDaddy for Web sites, and use comodo for code signing. Keys and other secrets are stored in Key Vault or LastPass.
C6	Describe your review and update process for your Security Policy and supporting security standards. a) How often do you review and update changes to your Security Policy, supporting security standards and Privacy Policy? b) Who performs the reviews and who approves the changes? c) How are these updates performed and how are they communicated to the organization?	Revisions to Security Policy are done ad hoc and not on a scheduled review process.
C7	Describe the process for exceptions to the Information Security Policy and supporting security standards. a) Who reviews and approves the exceptions? b) How often are existing exceptions reviewed?	Cyber Security reviews and approved security policy exceptions.
C8	Describe the security awareness training that you provide to employees, and when relevant, contractors and third party personnel. a) Who is trained and with what frequency? b) Are phishing email tests conducted and how often?	Security awareness training is done with onboarding and phishing awareness test are done periodically.
C9	Describe your risk review process for applications, infrastructure, network, etc. a) Is this a formal enterprise wide assessment process? b) Does it include likelihood and impact risk ratings? c) Are the results reviewed and risks accepted by business owners? Provide a copy of your Risk Management policy or standard.	Nathcorp has minimal internal infrastructure and primarily utilized Azure and M365. a) Cyber Security assesses risk as new applications or infrastructure are proposed b) Yes c) Yes, but standards and not documented
C10	Provide copies of the most current independent third party reviews of your company, attestations or audits of the systems and hosting providers (if applicable) that would process Sun Life information (SOC, SSAE18, CSAE3416, ISAE3402, PCI, etc.).	All Systems for the solution will be built in the Sun Life cloud or on-prem infrastructure.

D - Third Party Security Controls		
D1	Describe your third party (e.g. vendor/outsourcing) risk management process. a) Is this part of a formal enterprise process that is applied to all Third Parties? b) Does the process include likelihood and impact risk ratings? c) Are the results reviewed and risks mitigated or accepted by business owners? d) Do you have legal counsel review all contracts with third parties? e) *Where applicable,* do you have a Business Associates Agreement (BAA) in place with third parties? (Including hosting services, public (cloud) platforms, etc.) f) Do you require all Third Parties to sign Non-disclosure agreements that protect your customers' confidential information? g) Is this process completed before access is provided to Sun Life data? h) Describe the process to periodically re-evaluate the Third Party's security posture Provide a copy of your third party management policy or standard.	a) Third party contracts are reviewed my management and legal council. b) Yes c) Yes d) Yes e) N/A f) Yes g) Yes h) Contracts are reviewed as they are renewed
D2	For each third party that hosts, develops, or supports Sun Life information: a) Provide the name and address of the Third Party. b) Describe the services provided by that Third Party (e.g., managed service provider, co-location service, application service provider, data centre, etc.) c) Specify what security due diligence was conducted to ensure Sun Life Information will be secure in the hands of that Third Party d) When was the last due diligence process conducted on the Third Party? e) Is there an inforce contract with the Third Party and does it include security and privacy requirements to protect Sun Life data in a manner that is no less stringent than your requirements in the existing/proposed agreement with Sun Life? For example: Data center hosting, systems support, software development, professional services, media scanning, records storage, data destruction, etc.	a) Microsoft Canada – 1201-222 Bay St, Toronto On M5K 1E7 b) Hyperscale Cloud Provider (Data center hosting) c) https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security d) Same as above e) There are NDA's in place between Microsoft and all parties

E - Logical Access Control		
E1	Describe your process for granting and removing access rights of employees, contractors and Third Party users upon hiring, job role change, and termination. a) Describe how you maintain segregation of duties in the access provisioning process. b) Is a centralized identity management system in place?	Access is granted and removed when contracts or employment is started or terminated. a) HR determines when a user is active. IT Security enables access. b) All identities and identity management is consolidated into Azure AD

E - Logical Access Control			
	If yes, please provide the name of the centralized identity management system.		
E2	Describe your formal process to have management regularly review users' access rights. a) How often is this done? b) Who performs and signs-off on these reviews?	We are currently planning implementing User Access Reviews using Azure Premium. Currently it is an informal process.	
E3	Do all of your users have a unique identifier (user id) for their individual use only? If not, explain why users are not provided with a unique user ID?	All users have a unique ID for individual use.	
E5	For all systems/applications that currently process or may process Sun Life Information:	**Internal Systems / Applications**	**External / Web Facing Systems / Applications**
	a) Do you have a formal password policy?	N/A	N/A
	b) What are the password length and complexity requirements?	N/A	N/A
	c) How many invalid login attempts does it take to lock out an account?	N/A	N/A
	d) What password history is maintained to prevent the re-use of passwords?	N/A	N/A
	e) What is the password expiry/change frequency?	N/A	N/A
	f) How are orphan accounts or accounts with an extended period of inactivity handled?	N/A	N/A
	g) Describe your controls for privileged accounts if different from above.	N/A	N/A
	h) How are passwords reset?	N/A	N/A
	i) How do users identify themselves during password resets?	N/A	N/A
	j) If passwords are ever emailed, explain the process	N/A	N/A
	k) What are the session timeout policies and is re-authentication required?	N/A	N/A
E6	For privileged access: a) How do you restrict and control the allocation and use of privileged access on workstations, servers, and network devices? b) Are privileged, Administrator, and Root accounts stored in a password vaulting solution (e.g. CyberArk, etc.)? c) Are controls in place to log and monitor privileged sessions? d) How often do you conduct a review of all privileged/administrator accounts? Does this include orphan accounts? e) Who performs and signs-off on these reviews?	a) Most of our users are consultants or developers and have administrative rights to our workstation. We use the defender for M365 suite to reduce the risk. All accounts are MFA enforced. b) We use Privilege Access Manager, LastPass Enterprise, and Azure Key Vault c) We use the defender for M365 suite to reduce the risk. d) We are currently planning implementing User Access Reviews using Azure Premium. e) Currently it is an informal process.	
E7	For each system/application that processes Sun Life Information, describe how authentication and authorization is achieved (e.g., ID/PW, group membership, linked to Active Directory or local ID/PW).	The solution will use Azure AD and Modern Authentication.	

E - Logical Access Control		
E8	Can accounts be provisioned with Sun Life's Identity Management system through an API (e.g., Sailpoint Integration)?	Yes
E9	For your external facing systems can you accommodate? • ADFS (preferred) • Single-Sign-On (SSO) solution using SAML 2.0+ IDP • Alternative SSO solutions?	• Yes • Yes • Yes

F - Operations Management		
F1	Describe your process to identify all technology (hardware and software) assets and how you maintain an inventory of all important technology assets.	We use Intune, Azure AD, Conditional Access, and Defender for Endpoint to identify hardware and software assets.
F2	Describe your IT change management process. Does it cover all existing and new applications, systems, databases, infrastructure, services, operations and facilities?	We use the clients change management systems while developing, maintaining, and operating the client systems.
F3	Describe your process for deploying new devices. a) Do you have a standardized secure configuration baseline (process or template for all devices? b) How are processes/templates updated to reflect new patches and security requirements?	We deploy Workstations using Intune. a) Microsoft Endpoint manager – MDM Security Baseline for Windows 10 and later b) Updates are managed through Intune.
F4	Describe the procedures you have in place to control the installation of software on operational systems.	Microsoft Defender for Endpoint scans the devices for vulnerable and unwanted software.
F5	Describe your workstation hard drive encryption process. a) Are the hard drives for laptops encrypted? b) What is the encryption algorithm and key strength used? c) Provide the name of the software used to provide this encryption	BitLocker encryption is enforced with Microsoft Endpoint manager policies. a) Yes b) AES 256 c) BitLocker
F6	Describe how regular backups of all your information assets are performed. a) Where are the backups stored (e.g., same physical location, remote location or cloud provider)? If stored at a remote location, please identify the location and/or vendor. b) Are your backups encrypted? c) What is the encryption algorithm and key strength used?	a) The solution will use the Clients backup solutions and encryption standard b) The solution will use the Clients backup solutions and encryption standard
F7	Describe any email or network Data Loss Prevention (DLP) systems that are in place for sensitive data and include product name.	We use Microsoft Purview Data Loss Prevention
F8	Describe how you manage DLP for removable media including external hard drives, backup tapes, CD/DVD, memory sticks, etc. a) Are USB ports locked down so information cannot be transferred to removable media? Provide product name used for this. b) Are your staff able to transfer information to removable media unencrypted? Describe the exception process.	Solution will not have removable media

F - Operations Management		
F9	Describe the controls used to provide website content filtering and include product name.	Endpoints use Defender for Endpoint Web Filtering. Offices use ASA firewalls.
F10	Describe the controls you use to ensure the secure handling, transfer, and storage of hard copy documents.	Hard copies of document are stored in locked offices. All confidential HR and financial documents are stored at the office in a locked cabinet. Any documents that need to be transferred are done via scan through a private sector in office.
F11	Describe the processes in place to ensure secure disposal of Sun Life data (within the application, data repositories and backups) upon termination of services. Describe the configuration capabilities for defining this retention.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
F12	Describe how you securely dispose or shred both removable media (e.g., Hard drives, CD/DVD, memory sticks, etc.) and printed material. Provide the destruction standard that is being followed (NIST 800-88, DoD 5220.22-M) If performed by a third party, are certificates of destruction provided?	Printed materials are shredded in the office by HR or finance. Everything else is wiped clean first by our tech department and then disposed of at a e-waste disposal center or hard drive shredding center following NIST 800-88 standards. Certificates of destruction provided - Yes

G - Software Development Life Cycle				
G	Secure Development: a) Describe your secure coding practices. b) How they are integrated into your Software Development Life Cycle (SDLC)? c) Describe how OWASP Top 10 application risks are taken into account in the SDLC training and coding processes. d) Describe any training in secure coding that is delivered to your developers.	Solution is Low to No Code. All NathCorp coding follows Microsoft best practices and is reviewed before being merged into the codebase. We use the latest CI/CD platforms and leverage automated security scans when possible.		
G2	Describe how source code is managed and access to source code is restricted. Provide the product name(s) used to perform this function.	We use Git to manage our source code. Only the development team members have access to this. Visual studio Git plugin is used by the developers to authenticate and access the repository. There is a close watch on branching, forks done by the developers.		
G3	Describe how peer code review is performed.	This is a informal process, but enforced by the team leads. The team leads also perform code reviews.		
G4	Describe your application code security testing processes	**Static Code Testing**	**Dynamic Code Testing**	**Penetration Testing**
	a) Provide the name of the product name(s) used to perform these tests.	Manual	Manual	BreachLock
	b) Who performs these tests?	Internal testers	Internal testers	Third Party
	c) Are these tests performed on continuous basis as part of the SDLC process and as part of each software code release? If not done as part of each software code release how often are they done? What is your usual software release cycle?	Yes Our usual release frequency is monthly	Yes	Once a year, or as necessary

G - Software Development Life Cycle		
	d) Provide an executive summary of the most recent penetration test that includes date, scope and remediation plans for any medium or higher ranked issues.	Scheduled for this year next month
	e) Do these testing processes take into account OWASP Top 10?	Yes
	f) If you are developing code for Sun Life, please provide the most recent security scan report.	Coding will be needed based on the custom requirements during implementation
G5	Describe the process to remediate any findings from the above security testing processes. Describe the remediation timeline for any High / Medium / Low findings.	NA at this point in time
G6	Describe the controls in place to separate development, testing and production environments.	Dev, Testing and Prod environments are isolated environments with access control. There is a clear release management process to migrate from lower to higher environment. We use git to checkin and checkout code from the repo. For testing a package is pushed via Azure DevOps to Testing and to Prod after testing
G7	For software vendors, describe how you ensure that any software that is being provided to Sun Life is being regularly updated to maintain compatibility with current supported versions of the operating systems, middleware and other dependent software (e.g. Java, Flash, etc.).	All the development happens in Azure environment. So patch compatibilities are immediately noticed and fixed to move forward. The same applies to third party libraries. The solution architect also periodically review the external library dependencies and compatibility issues and address them based on criticality and urgency.

H - Application Security		
H1	Describe how Sun Life information will be separated / isolated from your other clients' information (i.e. application and database levels).	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
H2	What are the application session timeout and re-authentication policies?	The Solution will comply with Sun Life policies and standards
H3	Describe how Sun Life data is encrypted at rest (include all data repositories). Which algorithm(s) and key strength(s) are used? Provide the product name(s) used to provide the encryption.	The Solution will comply with Sun Life policies and standards
H4	Application Logging: a) Do all applications that handle Sun Life data generate audit logs? b) Is there any Sun Life confidential data stored in these logs? c) If yes, then can Sun Life confidential data be masked or obfuscated instead? d) How are the logs protected? e) How long are logs retained (online and offline/backup)? f) Who reviews the logs? g) How often are the logs reviewed? h) For applications installed at Sun Life, can the log data be exported to Splunk?	The Solution will comply with Sun Life policies and standards. Logs will be stored in Sun Life's SIEM or Log management solution.
H5	Is Sun Life data ever used in a non-production environment?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.

H - Application Security		
	a) If so under what situations? b) Describe any data masking techniques used.	

I - Network Security		
I1	Describe the solutions you have in place to mitigate the effects of Distributed Denial of Service (DDoS) attacks. a) Has your organization established a contract with a provider to manage DDoS attacks against your internet facing web services/systems? If yes, note the anti-DDoS service provider name and provide a high level description of the protections/configurations services purchased. b) Provide a description of any other DDoS attack mitigation measures that you have implemented at your organization. c) Provide the name of the DDoS provider.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant and utilize Sun Life's DDoS protection.
I2	Describe the network firewall and configuration used to protect confidential information. Provide the name of the firewall.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
I3	Describe the Intrusion Detection or Prevention System (IDS / IPS) (network or host based) and configuration used to protect confidential information. a) How often is it updated with new software or signatures? b) What is being monitored and alerted on? c) Provide the name of the product	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
I4	Describe how network access control (NAC) and/or or endpoint authentication is implemented as it relates to applications and systems used to provide the services to Sun Life.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
I5	Is a wireless network used in your organization? If so: a) Is there a corporate wireless network in place? Does this network have access to production systems that stores or process Sun Life confidential information? b) Is a guest wireless network in place? Is this network segregated from all other company networks? c) How are wireless network segments segregated from the company internal network using VLANs or other appropriate technologies? d) Provide the encryption algorithm and key strength for the wireless networks e) Are non-company owned devices permitted to connect to your wireless network? If so, indicate which wireless network and what security controls are in place.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
I6	Is there multi factor authentication for remote access to the corporate network from an external network? e.g., use of RSA token and VPN. If yes, describe the process and provide the name of the product. If not, explain your process for authentication for remote access.	Solution will support MFA. Azure AD MFA is the preferred control.

I - Network Security		
I7	Have you implemented IP whitelisting or SSO for connections from Third Parties? Have you implemented IP whitelisting or SSO for connections from Sun Life?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant. The Solution will comply with Sun Life policies and standards.

J - Threat and Vulnerability Management		
J1	Describe your security incident response process. a) How often are the security incident response plans tested? When was the last test performed? b) Describe the process to notify Sun Life of any security incident that impacts Sun Life or Sun Life clients?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant. The Solution will comply with Sun Life policies and standards.
J2	Describe your Information Security forensic capabilities.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant. NathCorp is partnered with Critical Start for Breach Response Services and Digital Forensic Investigations.
J3	Describe the detection, prevention, and recovery controls you have in place to protect against malicious code. a) What antivirus scanning software do you use? b) Is it centrally managed? c) Is it setup for real time, on-access scanning or both? d) How often is the software and the signatures updated? e) Which types of devices are being actively scanned and protected by the antivirus? f) Are email attachments scanned for malicious code? g) Are attachments uploaded via a web portal or application scanned for malicious code? h) Is antivirus scanning run on web applications that have file upload capabilities?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant. The Solution will utilize Sun Life's preferred malware protection and standards.
J4	Advanced Malware Protection (AMP) and Endpoint Detection and Response (EDR): a) Describe any AMP mechanisms you employ where suspicious code is executed and examined in a sandbox environment (e.g. FireEye, Cisco AMP, etc.). b) Does this AMP include behavioural analysis (not signature based) as the potential malware is being executed -or- execution of potential malware in a sandbox or virtual environment? c) Describe any EDR you employ where suspicious processes are inspected (e.g. Carbon Black, CrowdStrike).	NathCorp workstations and servers use Microsoft Defender for Endpoint and the Defender for M365 suite. The Solution will utilize Sun Life's preferred malware protection and standards.
J5	Describe your infrastructure security logging and review process. a) List what security events are logged for applications and key infrastructure components (e.g., Active Directory, Firewalls, IDS, Anti-	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.

J - Threat and Vulnerability Management			
	Virus, Servers, Database Admin) to ensure that all required activities are captured to support security investigations. b) Is there any Sun Life confidential data stored in these logs? If yes, then can Sun Life confidential data be masked or obfuscated instead? c) How do you protect the logging facilities and log information from tampering and unauthorized access on the originating systems? d) How long are logs retained (online and offline/backup)? e) Is there a manual process for regular review of the logs? i) Who reviews the logs? ii) How often are the logs reviewed? f) Are logs centralized, aggregated, correlated, and analyzed for anomalous patterns (e.g., Security Information and Event Manager – SIEM)? g) Which logs are sent to the SIEM? h) Provide the name of the SIEM product. i) Are automated alerts sent to key employees and is there a process to respond accordingly based on risk level?	a) The Solution will comply with Sun Life policies and standards. b) There will not be confidential data stored in logs. c) Logs will be stored in Sun Life's SIEM or Log management solution. d) Logs will be stored in Sun Life's SIEM or Log management solution. e) The Solution will comply with Sun Life policies and standards. f) Logs will be utilized Sun Life's SIEM or Log management solution. g) The Solution will comply with Sun Life policies and standards. h) Logs will be utilized Sun Life's SIEM or Log management solution. i) The Solution will comply with Sun Life policies and standards.	
J6	Describe integration capabilities for your applications and systems with other third party analytic or monitoring tools (such as SIEM, Splunk, Tableau, etc.). Describe the capability to make the contents of generated reports (such as audit trails, user activity monitoring, user-defined reports, chain-of-custody reports) available to external applications through APIs or other means.	The solutions will use standard log formats and can be ingested by any of the listed tools.	
J7	Describe your patch management process and execution of Zero Day patching processes, including frequency and scope. a) Does this cover all operating systems, devices and platforms (including network devices, vendor supplied appliances, etc.)? b) Does this cover all software, both commercial and open source? c) Provide the name of the product(s) used to provide these services. d) Provide remediation timelines based on severity level (High / Medium / Low).	The Solution will comply with Sun Life policies and standards.	
J8	Describe your vulnerability scanning practices:	**Internal / Infrastructure**	**External**
	a) What is the scope of these tests?	All servers and Workstations. Microsoft Defender Vulnerability Management provides continuous vulnerability scanning	Solution is serverless

J - Threat and Vulnerability Management			
	b) What is the frequency of these tests?	Continuous discovery and remediation tracking	Solution is serverless
	c) Who performs these tests?	This is an automated service	Solution is serverless
	d) Provide the name of the product(s) used to provide these services.	Microsoft Defender Vulnerability Management	Solution is serverless
	e) Provide remediation timelines based on risk level (High / Medium / Low).		

K - Mobile Device Management			
K1	Describe your formal mobile device policy. Does your employee training clearly define mobile devices (smartphones and tablets) and the accepted usage and requirements for mobile devices? Describe your change management process for mobile devices, including OS upgrades and updates.	Intune is used to manage Mobile devices and enforce compliance. We support BYOD and corporate owned devices. Intune polices enforce Windows Updates and minimum mobile OS versions.	
K2	Describe the applications and data accessed by the mobile devices. Specify if they will access Sun Life confidential data, what type data (such as PII, PHI, financial, contracts, etc.) and volume/frequency.	**Company owned devices**	**Bring Your Own Devices (BYOD)**
		The Solution will comply with Sun Life policies and standards.	The Solution will comply with Sun Life policies and standards.
K3	Describe your security controls for Mobile Device Management (MDM)	**Company owned devices**	**Bring Your Own Devices (BYOD)**
	a) Password policy	6 characters	6 characters
	b) Encryption	Required	Required
	c) Remote wipe	Enterprise Wipe	Enterprise Wipe
	d) Information segregation	App protection policies	App protection policies
	e) Provide the name of the product(s) used to provide these controls	Microsoft Intune.	Microsoft Intune.

L - Physical Security			
L1	For each type of location describe the physical security controls:	**Data Centre**	**Office Locations**
	a) How do you restrict physical access to information assets by users and support personnel? Describe the controls (passcodes, biometrics, mantraps, etc.)	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
	b) How are employees, contractors and building service staff authorized (i.e. approved) for access to each location?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
	c) How often is physical security access reviewed and by whom?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.

L - Physical Security			
	d) What is the process for authorizing and managing visitor access?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
	e) Do you have security guards in place and do they perform regular patrols?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.
	f) Do you have CCTV cameras in place for all ingress and egress point? How long are the CCTV recordings kept for?	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.	Sun Life data will be stored and processed at Sun Life's data center or Cloud tenant.