

VOYA DATA SECURITY ADDENDUM

1. Definitions.

“Affected Persons” means Client’s and its Affiliate’s former and current employees whose Personal Information (“PI”) may have been disclosed or compromised as a result of an Information Security Incident.

“Affiliates” means any entities that, now or in the future, control, are controlled by, or are under common control with Client. An entity will be deemed to control another entity if it has the power to direct or cause the direction of the management or policies of such entity, whether through ownership, voting securities, contract, or otherwise.

“Confidential Information” means (a) non-public information concerning the Disclosing Party, its affiliates, and their respective businesses, products, processes, and services, including technical, marketing, agent, customer, financial, personnel, and planning information; (b) PI; (c) trade secrets; and (d) any other information that is marked confidential or which, under the circumstances surrounding disclosure, the Non-Disclosing Party should know is treated as confidential by the Disclosing Party. Except with respect to PI, which will be treated as Confidential Information under all circumstances, Confidential Information will not include (A) information lawfully obtained or developed by the Non-Disclosing Party independently of the Disclosing Party’s Confidential Information and without breach of any obligation of confidentiality; or (B) information that enters the public domain without breach of any obligation of confidentiality. All Confidential Information will remain the property of the Disclosing Party.

“Information Security Incident” means any breach of security or cyber security incident impacting Voya that has a reasonable likelihood of (a) resulting in the loss or unauthorized access, use or disclosure of Client PI; (b) materially affecting the normal operation of Voya; or (c) preventing Voya from complying with all of the privacy and security requirements set forth in this Agreement.

“Law” means all U.S. and non-U.S. laws, ordinances, rules, regulations, declarations, decrees, directives, legislative enactments and governmental authority orders and subpoenas.

“Personal Information (PI)” means any information or data that (a) identifies an individual, including by name, signature, address, telephone number or other unique identifier; (b) can be used to identify or authenticate an individual, including passwords, PINs, biometric data, unique identification numbers (e.g., Social Security numbers), answers to security questions or other personal identifiers; (c) is “non-public personal information” as defined in the Gramm-Leach-Bliley Act 15 U.S.C. § 6809(4) or “protected health information” as defined in 45 C.F.R. § 160.103; (d) is an account number or credit card number or debit card number, in combination with any required security code, access code, or password, that would permit access to an individual’s financial account; or (e) is “Personal Information” as defined in The California Consumer Privacy Act of 2018 (Cal. Civ. Code Division 3, Part 4, Title 1.81.5).

“Services” means the services that Voya provides to Client pursuant to this Agreement.

“Voya Personnel” means Voya’s employees and subcontractors engaged in the performance of Services.

2. Data Security.

2.1. Security Standards and Controls.

- (a) Voya will establish and maintain:
 - (i) Administrative, technical, and physical safeguards against the destruction, loss, or alteration of confidential Information; and
 - (ii) Appropriate security measures to protect Confidential Information, which measures meet or exceed the requirements of all applicable Laws relating to personal information security.
- (b) In addition, Voya will implement and maintain the following information security controls:
 - (i) Privileged access rights will be restricted and controlled;
 - (ii) An inventory of assets relevant to the lifecycle of information will be maintained;
 - (iii) Network security controls will include, at a minimum, firewall and intrusion prevention services;
 - (iv) Detection, prevention and recovery controls to protect against malware will be implemented;
 - (v) Information about technical vulnerabilities of voya's information systems will be obtained and evaluated in a timely fashion and appropriate measures taken to address the risk;
 - (vi) Detailed event logs recording user activities, exceptions, faults, access attempts, operating system logs, and information security events will be produced, retained and regularly reviewed as needed; and
 - (vii) Development, testing and operational environments will be separated to reduce the risks of unauthorized access or changes to the operational environment.

2.2. Information Security Policies. Voya will implement and maintain written policies, standards or procedures that address the following areas:

- (a) Information security;
- (b) Data governance and classification;
- (c) Access controls and identity management;
- (d) Asset management;
- (e) Business continuity and disaster recovery planning and resources;
- (f) Capacity and performance planning;
- (g) Systems operations and availability concerns;
- (h) Systems and network security;
- (i) Systems and application development, quality assurance and change management;
- (j) Physical security and environmental controls;
- (k) Customer data privacy;
- (l) Patch management;
- (m) Maintenance, monitoring and analysis of security audit logs;
- (n) Vendor and third party service provider management; and
- (o) Incident response, including clearly defined roles and decision making authority and a logging and monitoring framework to allow the isolation of an incident.

2.3. Subcontractors. Voya will implement and maintain policies and procedures to ensure the security of Confidential Information and related systems that are accessible to, or held by, third party service providers. Voya will not allow any third parties to access Voya's systems or store or process sensitive data, unless such third parties have entered into written contracts with Voya that require, at a minimum, the following:

- (a) The use of encryption to protect sensitive PI in transit, and the use of encryption or other mitigating controls to protect sensitive PI at rest;
- (b) Prompt notice to be provided in the event of a cyber security incident;
- (c) The ability of Voya or its agents to perform information security assessments; and
- (d) Representations and warranties concerning adequate information security.

2.4. Encryption Standards, Multifactor Authentication and Protection of Confidential Information.

- (a) Voya will implement and maintain cryptographic controls for the protection of Confidential Information, including the following:
 - (i) Use of an encryption standard equal to or better than the industry standards included in applicable National Institute for Standards and Technology Special Publications (or such higher encryption standard required by applicable Law) to protect Confidential Information at rest and in transit over un-trusted networks;
 - (ii) Use of cryptographic techniques to provide evidence of the occurrence or nonoccurrence of an event or action;
 - (iii) Use of cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources; and
 - (iv) Development and implementation of policies on the use, protection and lifetime of cryptographic keys through their entire lifecycle.
- (b) In addition to the controls described in clause (a) above, Voya will:
 - (i) Implement multi-factor authentication for all remote access to Voya's networks;
 - (ii) Ensure that no Client PI is (A) placed on unencrypted removable media, mobile devices, computing equipment or laptops or (B) stored outside the United States; and
 - (iii) Ensure that media containing Confidential Information is protected against unauthorized access, misuse or corruption during transport.

2.5. Information Security Roles and Responsibilities. Voya will employ personnel adequate to manage Voya's information security risks and perform the core cyber security functions of identify, protect, detect, respond and recover. Voya will designate a qualified employee to serve as its Chief Information Security Officer ("CISO") responsible for overseeing and implementing its information security program and enforcing its information security policies. Voya will define roles and responsibilities with respect to information security, including by identifying responsibilities for the protection of individual assets, for carrying out specific information security processes, and for information security risk management activities, including acceptance of residual risks. These responsibilities should be supplemented, where appropriate, with more detailed guidance for specific sites and information processing facilities.

2.6. Segregation of Duties. Voya must segregate duties and areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of Voya's assets and ensure that no single person can access, modify or use assets without authorization or detection. Controls should be designed to separate the initiation of an event from its authorization. If segregation is not reasonably possible, other controls such as monitoring of activities, audit trails and management supervision should be utilized. Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

2.7. Information Security Awareness, Education and Training. Voya will provide regular information security education and training to all Voya Personnel, as relevant for their job function. In addition, Voya will provide mandatory training to information security personnel and require key information security personnel to stay abreast of changing

cyber security threats and countermeasures.

- 2.8. Vulnerability Assessments. Voya will conduct monthly vulnerability assessments that meet the following criteria:
- (a) All production servers and network devices must be scanned at least monthly;
 - (b) All vulnerabilities must be rated;
 - (c) All vulnerability remediation must be prioritized based on risk;
 - (d) All tools used for scanning must have signatures updated at least monthly with the latest vulnerability data; and,
 - (e) Voya will implement and maintain a formal process for tracking and resolving issues in a timely fashion.
- 2.9. Penetration Testing. If any Services to be provided by Voya include the hosting or support of one or more externally facing applications that can be used to access systems that store or process Client data, the terms of this Section will apply.
- (a) At least once every 12 months during the Term and prior to any major changes being moved into production, Voya will conduct a Valid Penetration Test (as defined below) on each internet facing application described above. As used herein, a "Valid Penetration Test" means a series of tests performed by a team of certified professionals, which tests mimic real-world attack scenarios on the information system under test and include, without limitation, the following:
 - (i) Information-gathering steps and scanning for vulnerabilities;
 - (ii) Manual testing of the system for logical flaws, configuration flaws, or programming flaws that impact the system's ability to ensure the confidentiality, integrity, or availability of client's information assets;
 - (iii) System-compromise steps;
 - (iv) Escalation-of-privilege steps; and
 - (v) Assignment of a rating for each issue based on the level of potential risk exposure to client's brand or information assets.
 - (b) Upon Client's request, Voya will provide to Client an executive summary of any material issues or vulnerabilities identified by the most recent Valid Penetration Test along with the scope of systems tested. The report may be redacted to ensure confidentiality.
- 2.10. Physical and Environmental Security. Voya will ensure that all sites are physically secure, including the following:
- (a) Sound perimeters with no gaps where a break-in could easily occur;
 - (b) Exterior roof, walls and flooring of solid construction and all external doors suitable protected against unauthorized access with control mechanisms such as locks, bars, alarms, etc.;
 - (c) All doors and windows to operational areas locked when unattended;
 - (d) Equipment protected from power failures and other disruptions caused by failures in supporting utilities;
 - (e) Closed-circuit television cameras at site entry/ exit points; badge readings at all site entry points, or other means to prevent unauthorized access; and
 - (f) Visitor sign-in/ mandatory escort at site; and
 - (g) With respect to remote work environments, if the foregoing controls are not present, then voya will use commercially reasonable efforts to mitigate any increased risk associated with such remote work environments, by, for example, limiting the types of access and functional roles eligible for a remote work environment, restricting access to a virtual private network (vpn) or virtual desktop infrastructure (vdi), providing formal guidance and standards for workspace security, and enhancing data protection controls such as data masking, logging and monitoring.
- 2.11. Information Security Incident Notification.

- (a) In the event of any Information Security Incident, Voya will, at its sole expense promptly (and in any event within 72 hours after Voya confirms an Information Security Incident) report such Information Security Incident to Client by sending an email to Client Contact Information, summarizing in reasonable detail the effect on Client, if known, and designating a single point of contact at Voya who will be:
 - (i) Available to Client for information and assistance related to the Information Security Incident; investigate such Information Security Incident, perform a root cause analysis, develop a corrective action plan and take all necessary corrective actions;
 - (ii) Mitigate, as expeditiously as possible, any harmful effect of such Information Security Incident and cooperate with Client in any reasonable and lawful efforts to prevent, mitigate, rectify and remediate the effects of the Information Security Incident;
 - (iii) Provide a written report to Client containing all information necessary for Client to determine compliance with all applicable laws, including the extent to which notification to affected persons or to government or regulatory authorities is required; and
 - (iv) Cooperate with Client in providing any filings, communications, notices, press releases or reports related to such Information Security Incident.
- (b) In addition to the other indemnification obligations of Voya set forth in this Agreement, Voya will indemnify, defend and hold harmless Client from and against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorneys' fees, arising out of or relating to any Information Security Incident, which may include, without limitation:
 - (i) Expenses incurred to provide notice to Affected Persons and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law;
 - (ii) Expenses related to any reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to, costs associated with the offering of credit monitoring or a similar identity theft protection or mitigation product for a period of at least twelve (12) months or such longer time as is required by applicable laws or any other similar protective measures designed to mitigate any damages to the Affected Persons; and
 - (iii) Fines or penalties that Client pays to any governmental or regulatory authority under legal or regulatory order as a result of the Information Security Incident.

2.12. Risk Assessments. Upon Client's request no more than once per year, Voya will complete an industry standard information security questionnaire and provide relevant Service Organization Control ("SOC") audit reports, when available. Voya's standard security requirements are set forth in Exhibit A. Voya represents and warrants that, as of the Effective Date, the statements in Exhibit A are true and correct in all material respects.

3. Privacy and PII.

3.1. With respect to any PI, Voya will:

- (a) Comply with the Voya Privacy Notice at www.voya.com/privacy-notice;
- (b) Retain, use, process and disclose all PI accessed, obtained or produced by Voya only to perform its obligations under this Agreement and as specifically permitted by this Agreement, or as otherwise instructed by Client, and not for any other purpose;

- (c) Refrain from selling such PI or using such PI for any other purpose, including for its own commercial benefit;
- (d) Treat all PI as Confidential Information;
- (e) Comply with the provisions of this Agreement to return, store or destroy the PI; and
- (f) Comply with all applicable Laws with respect to processing of PI.

Voya hereby certifies to Client that it understands the restrictions and obligations set forth above and will ensure that Voya and all Voya Personnel comply with the same.

- 3.2. As needed to comply with applicable Laws concerning the processing of PI or personal information security, or to the extent required by any changes in such Laws or the enactment of new Laws, the Parties agree to work cooperatively and in good faith to amend this Agreement in a mutually agreeable and timely manner, or to enter into further mutually agreeable agreements in an effort to comply with any such Laws applicable to the Parties. If the Parties cannot so agree, or if Voya cannot comply with the new or additional requirements, Client may terminate this Agreement upon written notice to Voya.

4. Confidential Information.

- 4.1. Confidential Information. Either Party ("Disclosing Party") may disclose Confidential Information to the other Party ("Non-Disclosing Party") in connection with this Agreement.
- 4.2. Use and Disclosure of Confidential Information. The Non-Disclosing Party agrees that it will disclose the Disclosing Party's Confidential Information only to its employees, agents, consultants, and contractors who have a need to know and are bound by obligations of confidentiality no less restrictive than those contained in this Agreement. In addition, Voya agrees that it will use the Disclosing Party's Confidential Information only for the purposes of performing its obligations under this Agreement. The Non-Disclosing Party will use all reasonable care in handling and securing the Disclosing Party's Confidential Information and will employ all security measures used for its own proprietary information of similar nature. These confidentiality obligations will not restrict any disclosure of Confidential Information required by Law or by order of a court, regulatory authority or governmental agency; provided, that the Non-Disclosing Party will limit any such disclosure to the information actually required to be disclosed. Notwithstanding anything to the contrary, Client may fully comply with requests for information from regulators of Client and the Client Affiliates.
- 4.3. Treatment of Confidential Information Following Termination. Promptly following the termination or expiration of this Agreement, or earlier if requested by the Disclosing Party, the Non-Disclosing Party will return to the Disclosing Party any and all physical and electronic materials in the Non-Disclosing Party's possession or control containing the Disclosing Party's Confidential Information. The materials must be delivered via a secure method and upon such media as may be reasonably required by the Disclosing Party.

Alternatively, with the Disclosing Party's prior written consent, the Non-Disclosing Party may permanently destroy or delete the Disclosing Party's Confidential Information and, if requested, will promptly certify the destruction or deletion in writing to the Disclosing Party. Notwithstanding the foregoing, if the Non-Disclosing Party, due to requirements of applicable Law, must retain any of the Disclosing Party's Confidential Information, or is unable to permanently destroy or delete the Disclosing Party's Confidential Information as permitted above within 60 days after termination of this Agreement, the Non-Disclosing Party will so notify the Disclosing Party in writing, and the Parties will confirm any extended period needed for permanent destruction or deletion of the Disclosing Party's Confidential Information. All Confidential Information in the Non-Disclosing Party's possession or control will continue to be subject to the confidentiality provisions of this Agreement. The methods used to destroy and delete the Confidential Information must

ensure that no Confidential Information remains readable and cannot be reconstructed so to be readable. Destruction and deletion must also comply with the following specific requirements:

MEDIUM	DESTRUCTION METHOD
Hard copy	Shredding, pulverizing, burning, or other permanent destruction method
Electronic tangible media, such as disks and tapes	Destruction or erasure of the media
Hard drive or similar storage device	Storage frame metadata removal to hide the organizational structure that combines disks into usable volumes and physical destruction of the media with a Certificate of Destruction (COD)

- 4.4. **Period of Confidentiality.** The restrictions on use, disclosure, and reproduction of Confidential Information set forth in this Section will, with respect to PI and Confidential Information that constitutes a “trade secret” (as that term is defined under applicable Law), be perpetual, and will, with respect to other Confidential Information, remain in full force and effect during the term of this Agreement and for three years following the termination or expiration of this Agreement.
- 4.5. **Injunctive Relief.** The Parties agree that the breach, or threatened breach, of any of the confidentiality provisions of this Agreement may cause irreparable harm without adequate remedy at law. Upon any such breach or threatened breach, the Disclosing Party will be entitled to injunctive relief to prevent the Non-Disclosing Party from commencing or continuing any action constituting such breach, without having to post a bond or other security and without having to prove the inadequacy of other available remedies. Nothing in this Section will limit any other remedy available to either Party.
5. **Cyber Liability Insurance.** During the Term, Voya will, at its own cost and expense, obtain and maintain in full force and effect, with financially sound and reputable insurers, cyber liability insurance to cover Voya’s obligations under this Addendum. Upon execution of the Agreement, Voya will provide Client with a certificate of insurance evidencing the following coverage and amount with such insurer:
- Risk Covered: Network Security (a.k.a. Cyber/IT)
Limits: \$50,000,000
6. **Disaster Recovery and Business Continuity Plan.** Voya maintains, and will continue to maintain throughout the Term, (a) a written disaster recovery plan (“Disaster Recovery Plan”), which Disaster Recovery Plan is designed to maintain Client’s access to services and prevent the unintended loss or destruction of Client data; and (b) a written business continuity plan (“BCP”) that permits Voya to recover from a disaster and continue providing services to customers, including Client, within the recovery time objectives set forth in the BCP. Upon Client’s reasonable request, Voya will provide Client with evidence of disaster recovery test date and result outcome.

Exhibit A

Security Requirements

FC: Foundation Controls	
FC-1:	Information Asset Management
FC-1.1	Voya implements and maintains an inventory list and assigns ownership for all computing assets including, but not limited to, hardware and software used in the accessing, storage, processing, or transmission of Client PI.
FC-1.2	Voya reviews and updates the inventory list of assets for correctness and completeness at least once every 12 months and updates the inventory list as changes are made to the computing assets.
FC-2:	Data Privacy and Confidentiality
FC-2.1	Voya will maintain an Information and Risk Management policy that is reviewed and approved by management at least annually.
FC-2.2	Voya protects the privacy and confidentiality of all Client PI received, disclosed, created, or otherwise in Voya's possession by complying with the following requirements:
FC-2.2A	Such information is encrypted at rest on mobile devices (including mobile storage devices), portable computers, and in transit over un-trusted networks with an encryption standard equal to or better than Advanced Encryption Standard (AES) 256 bit encryption or such higher encryption standard required by applicable law.
FC-2.2B	All hardcopy documents and removable media are physically protected from unauthorized disclosure by locking them in a lockable cabinet or safe when not in use and ensuring that appropriate shipping methods (tamper-proof packaging sent by special courier with signatures) are employed whenever the need to physically transport such documents and removable media arises.
FC-2.2C	All media is labeled and securely stored in accordance with Voya policies.
FC-2.2D	All electronic media is securely sanitized or destroyed when no longer required in accordance with industry standards.
FC-3:	Configuration Management
FC-3.1	Voya implements and maintains accurate and complete configuration details (e.g., Infrastructure Build Standards) for all computing assets used in accessing, storing, processing, or transmitting Client PI.
FC-3.2	Voya reviews configuration details of the computing assets at least once every 12 months to validate that no unauthorized changes have been made to the assets.
FC-3.3	Voya updates the configuration details of all computing assets used to access, process, store, or transmit Client PI as configuration changes take place.
FC-4:	Operating Procedures and Responsibilities
FC-4.1	<p>Voya implements and maintains operational procedures for information processing facilities and designates specific roles or personnel responsible for managing and maintaining the quality and security of such facilities, including, but not limited to, formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities.</p> <p>Voya IT policies and standards document the policies and procedures for job scheduling processes and tools.</p>
FC-4.2	Voya updates the operational procedures as changes take place and performs a comprehensive review and update of the procedures at least once every 2 years.

FC-5: Security Awareness and Training	
FC-5.1	Voya performs pre-employment background checks, including criminal history for 7 years, credit score and history (if applicable), credentials verification (if applicable), and educational background.
FC-5.2	Voya implements and maintains a documented security awareness program for all Voya Personnel which covers access to Client PI.
FC-5.3	Voya's security awareness program includes security requirements, acceptable use of computing assets, legal responsibilities, and business controls, as well as training in the correct use of information processing facilities and physical security controls.
FC-5.4	Voya ensures that all Voya Personnel complete security awareness training prior to being provided access to Client PI and at least annually thereafter. Voya provides mandatory annual training programs that include security awareness training to all Personnel.
UA: User Access Controls	
UA-1: User Access Controls	
UA-1.1	Voya implements and maintains identity management system(s) and authentication process(es) for all systems that access, process, store, or transmit Client PI.
UA-1.2	Voya ensures that the following user access controls are in place:
UA-1.2A	The "Least Privilege" concept is implemented ensuring no user has more privileges than they require in performing their assigned duties.
UA-1.2B	Users requiring elevated privileges as a normal part of their job responsibilities have a regular, non-privileged account to perform regular business functions.
UA-1.2C	All users have an individual account which cannot be shared
UA-1.2D	Account Names/IDs are constructed not to reveal the privilege level of the account or position of the account holder.
UA-1.2E	System- or application-level service accounts are owned by a member of management or an IT system administration delegate and only have the privileges necessary to function as required by the application, system, or database for which the account has been created.
UA-1.2F	Automated processes disable access upon 24 hours of termination and initiate manager review on employee position changes, in accordance with Voya policies.
UA-2: Access Control Management	
UA-2.1	Voya maintains a comprehensive physical security program. Access to Voya facilities is restricted and logs are maintained for all access. Physical security and environmental controls are present in Voya buildings.
UA-2.2	Voya ensures that access to systems that access, process, store, or transmit Client PI is limited to only those personnel who have been specifically authorized to have access in accordance with the users' assigned job responsibilities.
UA-2.3	Voya ensures that accounts for systems that access, process, store, or transmit Client PI are controlled in the following manner:
UA-2.3A	Users must provide a unique ID and Password for access to systems. Access to applications/systems is limited to a need-to-know basis, and is enforced through role based access controls.
UA-2.3B	Accounts are protected on computing assets by screen-savers that are configured with an inactivity time-out of not more than 15 minutes.
UA-2.3C	Accounts are locked after no more than 5 consecutive failed logon attempts, depending upon the system and platform.
UA-2.3D	Accounts remain locked until unlocked by an Administrator or through an approved and secure end-user self-service process.

UA-2.3E	Accounts are reviewed on a periodic and regular basis to ensure that the account is still required, access is appropriate, and the account is assigned to the appropriate user.
UA2.4	Voya ensures that wireless mobile devices are secured against threats coming from these wireless networks and wireless connections are required to be encrypted.
UA-3: User Access Management	
UA-3.1	Voya ensures that passwords for all accounts on systems that access, process, store, or transmit Client PI are configured and managed in accordance with industry standards:
UA-4: Information Access Restriction	
UA-4.1	Voya implements information access restrictions on all systems used to access, process, store, or transmit Client Information.
UA-4.2	Voya ensures the following Information Access Restrictions are in place:
UA-4.2A	Access to underlying operating systems and application features that the user does not require access to in the performance of their assigned responsibilities are strictly controlled.
UA-4.2B	Access to source code and libraries are restricted to only those individuals who have been specifically approved to have access. A person who develops code changes cannot be the same person who migrates the code change into production.
UA-4.2C	Access between Development, Test, and Production environments are strictly controlled. The version management system provides segregation of code, data and environments.
UA-4.2D	Temporary privileged access to production data is granted to authorized personnel based on job function for emergency support and only via access control and logging security tools.
PS: Platform Security Controls	
PS-1: Computer System Security (Servers and Multi-user Systems only)	
PS-1.1	Voya implements and manages a formal process for ensuring that all computer systems that access, process, store, or transmit Client PI are protected and configured as follows prior to and while remaining in a production status:
PS-1.1A	Systems are assigned to an asset owner within Voya's organization.
PS-1.1B	Systems are located in a data center or similarly controlled environment with appropriate physical security mechanisms and environmental controls to ensure systems are protected from theft, vandalism, unplanned outages, or other intentional or unintentional hazards.
PS-1.1C	All systems are configured to meet Voya standards, monitored to ensure a compliant state, and patched as required to maintain a high degree of security. Issues found to be out of compliance are required to be tracked to closure.
PS-1.1D	Systems are configured with commercially available and licensed anti-virus software which is set to perform active scans, perform scans of uploaded or downloaded data/files/web content, and is updated on at least on a daily basis.
PS-1.1E	System clocks are configured to synchronize with a reputable time source (e.g., NTP).
PS-1.1F	Systems display a warning banner to all individuals during the logon process that indicates only authorized users may access the system.
PS-1.1G	Systems that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.

PS-1.1H	All high and medium vulnerability and risk issues identified are remediated utilizing a risk based approach and in alignment with application team code release schedules.
PS-1.1I	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor systems.
PS-2: Network Security	
PS-2.1	To ensure systems accessing, processing, storing, or transmitting Client PI are protected from network related threats, Voya implements the following network security controls prior to connecting any network component to a production network and for the duration that the component remains in a production status.
PS-2.1A	Networks are constructed using a defense-in-depth architecture, are terminated at a firewall where there are connections to external networks, and are routinely scanned for unapproved nodes and networks.
PS-2.1B	Business-to-Business (B2B) and Third Party network connections (Trusted) to systems accessing, processing, storing, or transmitting Client PI are permitted only after a rigorous risk assessment and formal approval by Voya management. Network connections from un-trusted sources to internal resources are not permitted at any time.
PS-2.1C	Network components (switches, routers, load balancers, etc.) are located in a data center or a secure area or facility.
PS-2.1D	Voya systems are configured to provide only essential capabilities and restrict the use of any unneeded functions, ports, protocols and services.
PS-2.1E	Intrusion detection/prevention technologies, firewalls, and proxy technologies are implemented, monitored and managed to ensure only authorized and approved traffic is allowed within and between segments of the network.
PS-2.1F	Internal Voya wireless networks are configured with the most robust security standards available, including but not limited to, 802.11i/n, strong authentication, IP/MAC address filtering, firewall protection, and intrusion detection/prevention.
PS-2.1G	Wireless networks are not used to access Client Information unless the information is encrypted at either the file or transport level.
PS-2.1H	Network components that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-2.1I	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor network components.
PS-3: Generic Application and Database Security	
PS-3.1	Voya implements and maintains an application security certification and assurance process that ensures that all applications that access, process, store, or transmit Client PI provide the following:
PS-3.1A	Application and database design ensures security, accuracy, completeness, timeliness, and authentication/authorization of inputs, processing, and outputs.
PS-3.1B	All data inputs are validated for invalid characters, out of range values, invalid command sequences, exceeding data limits, etc. prior to being accepted for production. Voya implements static source code analysis tools to validate data inputs.
PS-3.1C	Application source code developed in house by Voya is protected through the use of a source code repository that ensures version and access control. The version management system provides segregation of code, data and environments.

PS-3.1D	Applications and databases are tested for security robustness and corrective measures are applied prior to the application being placed into a production environment. All systems are configured to meet Voya standards, monitored to ensure compliance state, and patched as required to maintain a high degree of security.
PS-3.1E	Applications and databases are implemented into a production environment with minimal privileges and critical configuration files and storage subsystems are protected from unauthorized access.
PS-3.1F	Applications and databases that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-3.1G	Voya ensures that Consumer/Internet facing applications have been designed and implemented using multi-factor authentication architecture. Web sessions require the use of an HTTPS (encrypted) connection, as well as authorization to approved data and services.
PS-3.1H	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor applications and databases.
PS-4: Workstation and Mobile Devices Security (End User Devices)	
PS-4.1	Voya ensures that the following security controls have been implemented and are maintained to protect Client PI accessed, processed, stored, or transmitted on workstations and mobile devices.
PS-4.1A	Workstations are located in a physically secure environment with mechanisms in place to prevent unauthorized personnel from accessing data stored on the device, reconfiguring the BIOS or system components, or from booting the device from unauthorized media. Portable devices are configured for boot-up encryption.
PS-4.1B	Laptops/portable computers and other mobile devices are assigned to an owner who is responsible for physically securing the device at all times, and the owner of the device must receive adequate awareness training on mobile device physical security.
PS-4.1C	Portable devices are configured for boot-up encryption. All laptop hard drives are encrypted using AES 256. Any device deemed "remote" requires hard drive encryption.
PS-4.1D	All workstations, laptops/portable computers and other mobile devices (where applicable) are configured with commercially available and licensed anti-virus software which is set to perform active scans, to perform scans of uploaded or downloaded data/files/web content, and is updated on at least a daily basis.
PS-4.1E	All workstations, laptops/portable computers and other mobile devices (where applicable) are configured with a commercially available and licensed operating system, patched according to manufacturer's recommendations, hardened according to best industry practices and standards and configured so that regular users do not have administrative privileges.
PS-4.1F	Laptops/portable computers and other mobile devices (where applicable) are configured with personal firewall technology.
PS-4.1G	Workstations, laptops/portable computers and other mobile devices (where applicable) display a warning banner to all individuals during the logon process that indicates that only authorized users may access the system or device.
PS-4.1H	Voya implements and maintains processes for recovering laptops/portable computers and mobile devices from terminated Voya Personnel.
PS-5: Backup and Restore	
PS-5.1	Voya implements and maintains backup and restore procedures to ensure that all Client PI received, disclosed, created, or otherwise in the possession of Voya is appropriately protected against loss.

PS-5.2	Voya ensures that backups are securely stored and storage systems are physically and logically protected.
PS-5.3	Voya implements a backup and availability schedule to meet business and regulatory requirements.
PS-6: Remote Network Access Controls	
PS-6.1	Voya implements and maintains a remote network access control strategy or process.
PS-6.2	Voya ensures the following remote network access controls are in place:
PS-6.2A	Users requiring remote access are appropriately authorized by Voya management.
PS-6.2B	Remote access connections are established through the use of Virtual Private Networking (VPN) or secure VDI mechanisms that provide transmission security, encryption and connection timeout (e.g. split-tunneling disabled.)
PS-6.2C	Only Voya approved and controlled (managed) computing devices are used when remotely accessing (where applicable) Voya's computing environments where Client PI is held. Any device deemed "remote" requires data encryption. Encrypted communications are required for all remote connections.
PS-6.2D	Users are thoroughly authenticated using multi-factor authentication prior to being provided remote access.
ITR: IT Resilience Controls	
ITR-1: Architecture	
ITR-1.1	Voya ensures that the architecture of computing environments where Client PI is accessed, processed, stored, or transmitted incorporates reasonable industry best practices for authentication/authorization, monitoring/management, network design, connectivity design, firewall and intrusion prevention technologies and storage and backup capabilities.
ITR-2: Hardware and Software Infrastructure Resilience	
ITR-2.1	<p>Voya ensures all hardware and software components classified with an availability rating of "critical" used in the accessing, processing, storage, or transmission of Client PI is:</p> <ul style="list-style-type: none"> • Identified and cataloged • Supported by the manufacturer of the component (or if developed in-house, follows Voya's SDLC Policy which includes quality/security) • Applications and systems classified as A4 may be designed with high availability features and have no single point of failure • Reviewed on a regular basis for capacity implications (at minimum once every 12 months)
ITR-2.2	Voya maintains Business Continuity Plans to address business unit and departmental actions to be undertaken before, during and after an incident or disaster. Voya's Disaster Recovery Plan addresses the recovery and availability of systems and data.
ITR-3: Capacity Assurance	
ITR-3.1	Voya ensures that computing environments used to access, process, store, or transmit Client PI are assessed for capacity and performance on a periodic basis (at minimum once every 12 months) and appropriate corrective actions are taken to make the environment sufficiently robust enough to perform its stated mission.
CM: Change Management Controls	
CM-1: Change Management Process	
CM-1.1	Voya implements and maintains a change control process to ensure that all changes to the environment where Client PI is accessed, processed, stored, or transmitted is strictly documented, assessed for impact, and approved by personnel authorized by Voya to provide approval for such changes, thoroughly tested, accepted by management, and tracked.

CM-1.2	Voya implements an emergency change control process to manage changes required in an emergency situation where a computing system is down or there are imminent threats/risks to critical systems involving Client PI.
CM-2: Separation of Environments	
CM-2.1	Voya maintains physically and/or logically separate development, test, and production computing environments. Development, testing, and acceptance environments are separate from the production environment.
CM-2.2	Voya ensures that Client data used for development or testing purposes is completely depersonalized/desensitized of confidential values prior to entering a development or test environment. Data is depersonalized in non-production controlled environments for testing purposes with required approvals. PI elements are required to be depersonalized in non- production environments.
SM: Security Monitoring Controls	
SM-1: Security Event Monitoring and Incident Management	
SM-1.1	Voya implements and maintains a security event monitoring process and associated mechanisms to ensure events on computing systems, networks, and applications that can impact the security level of that asset or the data residing therein are detected in as close to real-time as possible for those assets used to access, process, store, or transmit Client PI.
SM-1.2	Voya implements and maintains an incident management process to ensure that all events with a potential security impact are identified, investigated, contained, remediated, and reported to Client effectively and in a timely manner.
SM-1.3	Voya has implemented monitoring controls that provide real-time notifications of events related to loss of confidentiality, the integrity, or the availability of systems.
SM-1.4	Event logs (audit trails) are stored for analysis purposes for a minimum period of 3 years.
SM-2: Technical State Compliance	
SM-2.1	Voya ensures computing environments that access, process, store, or transmit Client PII are continually in compliance with quality and security requirements including, but not limited to, authentication/authorization, monitoring/management, network design, connectivity design, firewall and intrusion prevention technologies, and storage and backup capabilities.
SM-2.2	Voya ensures IT Risk Management facilitates risk assessments of information technology processes and procedures in accordance with the annual IT Risk Assessment Plan approved by the IT/Privacy Risk Committee. Risk Assessment results are communicated to management for awareness and resolution or risk acceptance of findings based on management's risk appetite.
SM-3: Security and Penetration Testing	
SM-3.1	Voya implements and maintains vulnerability and penetration testing (Ethical Hacking) processes to ensure the computing environment where Client PII is accessed, processed, stored, or transmitted is continually protected from internal and external security threats.
SM-3.2	Voya implements and maintains a process for vulnerability scanning on at least a monthly basis and ensures issues are remediated, utilizing a risk based approach within a reasonable timeframe.
SM-3.3	Penetration testing (Ethical Hacking) of Internet facing systems or systems exposed to un- trusted networks is conducted prior to the system being deployed into a production status, after any significant changes, and then at least once every 12 months thereafter.