Supplier Security Standard

Effective Date: March 1, 2019

Table of Contents

1.0 Introduction and Purpose

New York Life has developed this Supplier Security Standard (the "**Standard**") to help its entire Supplier community protect and maintain the Confidentiality, Integrity, and Availability of New York Life's data and information technology environment. Capitalized terms used in this Standard are defined in their immediate context or in Section 5.0 (Glossary).

The Standard provides the minimum security requirements that all Suppliers must adopt to ensure that Scoped IT Assets are protected from unintentional or malicious alteration. Supplier's providing Hosted Solutions and Outsourced Delivery Center (ODC) services must also fully comply with Sections 3 and 4 (Hosted Solutions Requirements and Outsourced Delivery Center Security Requirements, respectively) of this Standard. In the event of any conflict between the general requirements of this Standard and the Hosted Solutions or ODC requirements, Hosted Solutions and ODC Suppliers will comply with the more stringent requirements.

Supplier's failure to meet the Standard may expose New York Life, its employees, customers, and business partners to risk, and result in harm to New York Life including financial loss, service disruptions, regulatory sanctions, and reputational damage. New York Life requires all Suppliers, including Supplier Personnel and Subcontractors, who are engaged in the provision of products and services to New York Life or who otherwise manage, operate, interact with, or have access to Scoped IT Assets, to meet the Standard.

This Standard supplements (1) the Supplier's agreement(s) with New York Life, and (2) other New York Life policies. If there are conflicts or inconsistencies among the Standard, Supplier's agreement with New York Life, or a New York Life policy, New York Life expects Supplier to comply with the terms that provide the greatest level of protection for New York Life and the Scoped IT Assets.

Note: Insurance-Related Servicers are covered by requirements defined in the New York Life Insurance-Related Servicers Security Standard.

2.0 Supplier Security Requirements

2.1 Comprehensive Security Program & Practices

2.1.1 Supplier must adopt, implement, maintain, review, and follow a comprehensive written security program designed to protect the Confidentiality, Integrity, and Availability of Scoped IT Assets.

2.1.2 Supplier must regularly perform risk assessments that include (1) identification of all Scoped IT Assets, (2) criticality or sensitivity of each Scoped IT Asset, (3) extent to which Supplier must use or access each Scoped IT Asset in the performance of its obligations for New York Life, (4) assessment of all controls related to Supplier's security program, and (5) requirements from industry standards and frameworks.

2.1.3 At a minimum, Supplier's security program must address the following areas (as applicable to the Scoped IT Assets and to Supplier's obligations to New York Life):

1. Data governance and classification;

2. Access Controls and identity management;
3. Business continuity and disaster recovery planning;
4. Capacity and performance planning;
5. Systems operations and Availability concerns and related elements such as network security, network monitoring, and defensive measures;
6. Physical security and environmental controls;
7. Customer data privacy;
8. Vendor and third-party service provider risk management;
9. Asset inventory and device management;
10. Systems and application development and quality assurance;
11. Incident response processes and procedures; and
12. Documented and distributed disciplinary policy for violation of security program.

2.1.4 The Supplier's security program must be approved by a senior officer of Supplier (e.g., a C-level executive or his or her direct reports) who has oversight over cybersecurity.

2.1.5 Supplier must provide written notice to New York Life if Supplier makes any changes to the Supplier's security program that reduce, weaken or lessen the requirements or obligations in the security program.

2.2 Supplier Personnel

2.2.1 Supplier must ensure that its security program (including its cyber security and privacy policies) is published and effectively communicated to all Supplier Personnel. Supplier must develop, document, and maintain security awareness, education, and other training to ensure that all Supplier Personnel fully understand their individual responsibilities and corporate security mandates, including Supplier's security program.

2.2.2 Supplier must ensure that all Supplier Personnel have certified in writing that they have reviewed and will comply with Supplier's security program, specifically those components that relate to Supplier's customers and those customer's data (in the case of New York Life as customer, the Scoped IT Assets).

2.2.3 Supplier must employ or retain Supplier Personnel as needed to effectively manage Supplier's security risks (cyber or otherwise) and to perform core cyber security functions.

2.2.4 Supplier must provide for and require Supplier Personnel engaged in performing cybersecurity functions to attend regular cybersecurity updates and training sessions aligned to prevailing standards for the financial services and insurance industry.

2.2.5 Supplier must conduct identity verification, work authorization, reference checks, and criminal background checks in accordance with New York Life policies and Applicable Laws (collectively, the "Pre-Assignment Checks") on all Supplier Personnel who have access to

Scoped IT Assets or are otherwise engaged in the provision of products or services to New York Life.

2.2.6 Supplier must not assign to New York Life, or retain on assignment to provide services to New York Life, any Supplier Personnel who (1) did not successfully pass the Pre-Assignment Checks, or (2) Supplier knows, suspects, or has reason to believe has been convicted of, pled guilty to, or participated in a pretrial diversion for, a crime involving dishonesty, breach of trust, money laundering, or any other similar type of crime.

2.2.7 Supplier must ensure that departing or terminated Supplier Personnel return all Scoped IT Assets to Supplier on or before Supplier Personnel's last day of employment. As part of its documented processes for the termination or departure of Supplier Personnel, immediately following termination or departure of Supplier Personnel that had access to Scoped IT Assets, Supplier must (1) cancel/remove such Supplier Personnel's access to Scoped IT Assets, including revocation of access to Supplier Systems, and (2) notify New York Life of the name of such Supplier Personnel.

2.2.8 Supplier must ensure that Supplier Personnel assigned to, or interact with, New York Life, consent to New York Life's requirements related to the collection, storage, processing, and dissemination or use of Personal Data pertaining to those Supplier Personnel.

2.2.9 Supplier must ensure there is no sharing of tokens, user IDs, passwords or any other similar information with and between any persons (including with and between Supplier Personnel) under any circumstances. Appropriate auditable break-glass procedures must be in place for New York Life approved emergency accounts.

2.3 Duty of Care & Use Restrictions

2.3.1 Supplier must adopt, maintain and follow risk-based security practices and procedures to safeguard Scoped IT Assets from the following:

1. Unauthorized disclosure, access, use, or modification;
2. Misappropriation, theft, destruction, or loss;
3. Anticipated threats or hazards to Confidentiality, Integrity and Availability;
4. Inability to account for the whereabouts or disposition.

2.3.2 Supplier must collect, store, process, disseminate and use New York Life Data:

1. Only as expressly instructed in writing by New York Life;
2. For the sole purpose of delivering products/services to New York Life, and only to the extent strictly necessary to do so;
3. In accordance with Applicable Laws, and New York Life policies.

2.3.3 Supplier must recertify access privileges for Scoped IT Assets granted to Supplier Personnel at least semi-annually (or at a lesser frequency as approved in writing by New York Life), based on Supplier's Risk Assessment.

2.3.4 Supplier must provide New York Life with the list of Supplier Personnel who have access to Scoped IT Assets and other required data fields to support New York Life's recertification process.

2.3.5 Supplier must adopt, implement, maintain, and follow procedures to remain apprised of, responsive to, and in full compliance with Applicable Laws.

2.3.6 Supplier must make modifications to Supplier's security program to ensure full compliance with all Applicable Laws, and to further ensure that Supplier's security program keeps pace with best standards and practices.

2.3.7 Unless prohibited under Applicable Laws, Supplier must promptly notify New York Life of any request to release any New York Life Data, and then may only disclose that portion of New York Life Data that has been approved for disclosure by New York Life.

2.4 Return/Destruction/Maintenance of Scoped IT Assets

2.4.1 Supplier must develop, implement, maintain, review and monitor ownership, inventory, return, and acceptable uses of Scoped IT Assets.

2.4.2 Supplier must develop, implement, maintain, and monitor procedures and controls for the secure handling, transfer, destruction, and disposal of Scoped IT Assets in any form.

2.4.3 Supplier must obtain written approval for allowing Supplier Personnel to access Scoped IT Assets through personal devices. Notwithstanding the foregoing, any personal devices used to access Scoped IT Assets, whether approved or not, are deemed to be part of Supplier's Systems.

2.4.4 Supplier must dispose of Scoped IT Assets in a way so that it may not be decoded, read, accessed, or decompiled.

2.4.5 Supplier must have the ability to comply with New York Life record management requirements (as communicated to Supplier) including holds, searches, retrievals, and timely destruction.

2.5 Physical Security

2.5.1 Supplier must maintain all Scoped IT Assets in secure facilities owned, operated, or contracted for by Supplier or in similarly secure manner for portable Scoped IT Assets (e.g. laptop computers, removable media, or mobile devices).

2.5.2 Supplier must limit access to and within its facilities (e.g. to Supplier Systems) to those Supplier Personnel with job-related needs and appropriate authorization, consistent with Supplier's risk assessment.

2.5.3 Supplier must monitor access to its facilities using measures that may include security guards, surveillance cameras placed to monitor entry and exit points, specifically capturing badge access, authorized entry systems, or similar methods capable of recording entry and exit information, consistent with Supplier's risk assessment. Logs detailing access must be stored for a minimum period of three years (to the extent permitted by Applicable Laws).

2.5.4 Supplier must maintain environmental controls at all facilities hosting Scoped IT Assets. The environmental controls may include, by example and not limitation, climate control (temperature and humidity), raised floor, smoke detector, heat detector, fluid sensor, CCTV, fire suppression, uninterrupted power supply, fire extinguisher equipment.

2.5.5 Supplier must maintain all backup and archival media related to Scoped IT Assets in secure, environmentally-controlled storage areas owned, operated, or contracted for by Supplier in accordance with New York Life's retention instructions.

2.6 Network & Communications Security

2.6.1 Supplier must deploy multiple layers of defense on Supplier Systems, including but not limited to firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS), consistent with Supplier's risk assessment. Supplier must also actively monitor Supplier Systems consistent with its risk assessment.

2.6.2 Supplier must configure network-related components of Supplier Systems (e.g. firewalls, network routers, switches, load balancers, domain name servers, mail servers) in accordance with its risk assessment and generally accepted information security standards in Supplier's industry and the insurance, investment, and financial services industries.

2.7 Infrastructure/Platforms/Services/Desktop/Operations Security

2.7.1 Supplier must ensure that all remote administrative access to production systems that are also Scoped IT Assets is performed over encrypted connections (e.g. SSH, SCP, SSL-enabled web management interfaces, and VPN/VDI solutions), utilizing the applicable Approved Encryption.

2.7.2 Supplier must implement desktop controls that include, by example and not limitation: (1) restricting End Users from being granted local administrator-level privileges, (2) disabling key desktop settings (e.g. screen saver, anti-virus) so that End User cannot alter those settings, (3) prohibiting and preventing New York Life Data from being stored on the local desktop, and (4) blocking peripheral devices (e.g., CD, DVD, USB drives).

2.7.3 Supplier must use Risk-Based Authentication when granting access to Scoped IT Assets not originating within Supplier Systems.

2.7.4 Supplier must use Multi-Factor Authentication for any access to Scoped IT Assets (including its accounts on Amazon Web Services (AWS), Microsoft Azure, and other cloud service providers) not originating within Supplier Systems.

2.7.5 All New York Life Data, including backup and archive copies, must be encrypted at rest using Approved Encryption.

2.7.6 All New York Life Data must be encrypted in transit using Approved Encryption.

2.7.7 Supplier must ensure that any changes to Supplier Systems are documented via formal change management procedures. Supplier must provide separate development, test, and production environments within Supplier Systems. Changes must be fully validated in one environment before being migrated to the next higher environment.

2.7.8 Supplier must ensure that all system clocks for Supplier Systems are synchronized with a single reference time source.

2.7.9 Supplier must use reasonable efforts to monitor, on a regular basis, reputable sources of computer security Vulnerability information such as FIRST, CERT/CC, and vendor mailing lists and take appropriate timely measures to obtain, test, apply, and provide relevant service packs, patches, upgrades, and workarounds to any software.

2.7.10 Supplier must maintain access, activity, and audit logs for changes to Supplier infrastructure/platforms/services, including tracking of both access attempts and privileged access to Scoped IT Assets, in accordance with New York Life's retention instructions and Applicable Laws.

2.7.11 Supplier should frequently develop and issue patches for its proprietary products, and deploy patches for third-party components of Supplier Systems as provided by the third-party provider, to correct problems, improve performance, and enhance security of Supplier Systems.

2.7.12 Supplier must implement time out and termination of system communication sessions and security sessions or contexts after a mutually agreed upon period of user inactivity.

2.8 Additional Software Provisions

2.8.1 Supplier must ensure, and upon New York Life's written request, provide New York Life with written certification that all software provided to New York Life (or otherwise leveraged or utilized by Supplier in the provision of products and services to New York Life) is not susceptible to the most recently published OWASP top 10 vulnerabilities (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project). The certification must confirm that Supplier has conducted or has had conducted on its behalf a static and dynamic code/program analysis that confirmed the absence of any bugs or flaws, including by way of example and not limitation, buffer overflows/underflows, NULL pointer dereferences, resource leaks, or any other reliability or security problem. All such tests must be done at least annually as well as upon issuance of a major upgrade.

2.8.2 Supplier must have an established development lifecycle for the purpose of defining, acquiring, developing, enhancing, modifying, testing or implementing Supplier Systems.

2.8.3 For software deliverables being developed by Supplier for New York Life, Supplier must adhere to the following:

1. Adhere to the New York Life Technology Delivery Lifecycle (TDLC) standards and artifact requirements.
2. To the extent that the New York Life TDLC does not address a particular issue or cannot be followed without material additional effort or expense, provide a documented Software Security Development Life Cycle (SSDLC) and proof of adherence to the SSDLC.
3. Provide a written set of security requirements and coding guidelines that indicate how developed code will be created, formatted, structured, tested and commented by Supplier.
4. Ensure that all developed code will be reviewed and validated by a documented process and tested against the security requirements and coding guidelines before Supplier provides the software deliverable to New York Life for any additional testing or review.
5. Identify the key risks to other Scoped IT Assets arising through the intended operation of the software, including risks to their Confidentiality, Availability, Integrity and Accountability, and develop appropriate controls to mitigate or minimize those risks.
6. Conduct an analysis of the CWE/SANS Top 25 Most Dangerous Software Errors or most common programming errors and provide New York Life with written documentation evidencing that any such errors have been fully mitigated and resolved.

2.9 Identity and Access Management

2.9.1 Supplier must ensure End User access capabilities for Scoped IT Assets are granted on a need-to-know basis.

1. Privileges must be consistent with assigned job responsibilities and must be configured with Least Privilege.
2. Supplier must clearly define the extent to which administrative or super user accounts may have access to Scoped IT Assets and the security controls in place to prevent misuse.

2.9.2 Supplier must implement operating system Access Controls that protect Scoped IT Assets from compromise. Protections must include but are not limited to appropriate authorization and management of all Scoped IT Assets.

2.9.3 Supplier must have a process workflow in place, including an approval process, to request, change, and remove End User access to Scoped IT Assets in a timely manner.

2.9.4 Supplier must maintain and adhere to procedures that restrict End User access to information and application functions and prevent and detect unauthorized access to Scoped IT Assets.

2.9.5 For Supplier-developed software deployed on New York Life's private network:

1. All End User identities must be managed by New York Life within the New York Life Corporate Directory.
2. All authentications of End User identities must be done via a New York Life approved method (currently AD/LDAP/Site Minder or SAML 2.0), as determined during the software requirements and design phase.
3. All End User authorization must take place through a New York Life approved platform (currently Directory, ACF2, and home grown).

2.9.6 Supplier must employ multi-layered controls to protect New York Life and its clients from unauthorized access to Scoped IT Assets. These controls must include an authentication protocol governing the requirements for End Users to access Scoped IT Assets, as well as additional fraud prevention controls to prevent unauthorized access such as disbursement limits, guidelines around High Risk Transactions (as defined by New York Life), and fraud monitoring.

2.10 Log Files

2.10.1 Supplier must adopt and operate systems to track and maintain all records, data, and schedules that allow for the complete and accurate reconstruction of all material financial transactions for at least the past five years to support normal operations.

2.10.2 Supplier must maintain, for a period of at least four years (or longer as may be required by Applicable Laws or contract), detailed log files (for audit trail) concerning all activity on Scoped IT Assets, to enable Supplier to detect and respond to a Security Incident. At a minimum, the following logs must be available in a machine-readable format, and protected against unauthorized access, modification, or deletion:

1. All End User sessions established, including user ID and date/time of authentication;
2. Roles assigned to the ID within solution at any point in time;
3. Actions performed by the ID when accessing the Scoped IT Asset;
4. Information related to the reception of specific information from an End User or from another system;
5. Failed authentication attempts for End Users;
6. Unauthorized attempts to access the Scoped IT Asset in whole or in part;
7. Administrator and operator actions;
8. Events generated (e.g., commands issued) to make changes in security profiles, permission levels, application security configurations, and/or system resources; and
9. Provisioning and deprovisioning of End Users and Scoped IT Assets.

2.11 Vulnerability Assessment and Penetration Testing

2.11.1 Supplier must test the implementation of its information security measures (including Supplier's security program) as applied to its Scoped IT Assets through the use of Vulnerability scanning tools and penetration testing, including monitoring, periodic penetration testing (which may include phishing and social engineering campaigns), and Vulnerability assessments.

2.11.2 Vulnerability Assessment

a) At least quarterly, Supplier must conduct a Vulnerability assessment by running authenticated scans from a scanning tool against Supplier Systems.

b) Supplier must mitigate all Critical/Very High/High Vulnerabilities (e.g., as defined in CVE or similar assessment standards) identified during the Vulnerability assessment by working diligently and continuously after learning of the Vulnerability until the Vulnerability has been remediated (which remediation will not exceed 30-days unless such longer period of time has been approved by New York Life). Vulnerabilities of a lower order should be remediated within 60 days.

c) To the extent the Supplier has identified areas, processes, or elements of or related to Supplier Systems that require material improvement, updating or redesign, Supplier must document the identification and the remedial efforts planned and underway to address such items. Summary documentation of these plans must be available for inspection by New York Life.

d) If New York Life elects to conduct its own Vulnerability assessment or ethical hack, Supplier must permit, and release from liability, New York Life and any third-party specialists retained by New York Life to perform the Vulnerability assessment or ethical hack.

2.11.3 Penetration Testing

a) At least annually, Supplier must perform penetration tests of all Scoped IT Assets. Supplier must share summary results of risk ranked Vulnerability status with New York Life on request.

2.12 Location of New York Life Data

2.12.1 Supplier must not store New York Life Data in, or export New York Life Data to, a location outside the United States (or the country of origin), without first obtaining written approval from New York Life and any required license or approvals under Applicable Laws, and then only in accordance with controls and security methods as approved by New York Life.

2.13 Subcontractors

2.13.1 Supplier must conduct risk assessments on Subcontractors in line with the risk that the Subcontractor may pose to the Supplier or New York Life.

2.13.2 For any Subcontractors of Supplier with access to or responsibility for Scoped IT Assets, Supplier must:

1. ensure that its contracts with those Subcontractors permit New York Life, its regulators, and their respective auditors to have access to the books and records of each Subcontractor;
2. audit its Subcontractors at least once every 12 months to ensure that each Subcontractor is in full compliance with Supplier's obligations and responsibilities under this Standard, including review of the Subcontractor's own annual audits (if any) under SSAE 18 (or any successor authoritative guidance for reporting on service organizations) and AT-101 or ISO/IEC 27001:2013 (or any successor information security standards), including substantive review of the effectiveness of such controls;
3. provide New York Life with written certification promptly after its completion of each audit, either confirming that the Subcontractor is in full compliance or identifying any non-compliance by the Subcontractor and a corrective action plan; and
4. provide New York Life with a copy of the results of each Subcontractor audit at New York Life's request.

2.14 Security Incident Management

2.14.1 Supplier must develop, implement, document, and maintain a process to ensure consistent identification, reporting, investigation, and closure of Security Incidents.

2.14.2 As part of its cyber security program, Supplier must establish a written incident response plan designed to promptly detect, respond to, and recover from, any Security Incident.

2.14.3 Supplier's incident response plan must, at a minimum, address the following areas:

1. Internal management processes for responding to a Security Incident;
2. Detail incident severity definitions consistent with New York Life 's Policies;
3. Set specific escalation procedures and timeframes based on the breach severity level of the Security Event;
4. Goals of the incident response plan;
5. Definitions of clear roles, responsibilities and levels of decision-making authority;
6. External and internal communications and information sharing;
7. Remediation of any identified weaknesses in Information Systems and associated controls;
8. Documentation and reporting regarding a Security Incident and related incident response activities; and
9. Evaluation and revision of the incident response plan following a Security Incident.

2.14.4 Supplier may not make or permit any statements concerning any Security Incident to any third-party without the advance, explicit, written authorization of New York Life's Office of The General Counsel.

2.14.5 As part of its cyber security program, Supplier must establish a written incident response plan designed to promptly detect, respond to, and recover from, any Security Incident.

2.14.6 In the event of a Security Incident, the Supplier must provide the following to New York Life:

1. A notification of the Security Incident promptly after the occurrence (but in all instances no more than 24 hours after the occurrence), followed by regular status updates, including but not limited to actions taken to resolve the Security Event, at four-hour intervals (or at other mutually agreed intervals or times) for the duration of the Security Event.
2. As soon as available (and updated throughout the Security Incident), a thorough description of the Security Incident, including the name(s) of any affected individual(s), the dates on which the Security Incident occurred and was discovered, type(s) of information implicated (and whether or not such information included New York Life Data), and, if the information was computerized data, whether the information was encrypted or protected by any other method or technology that renders the electronic files, media, or databases unreadable or unusable.

3. Full cooperation and assistance to New York Life in responding to the Security Incident; and
4. Within three days of the closure of the Security Incident, a written report describing the Security Incident, actions taken by Supplier during its response thereto, and Supplier's action plan to prevent similar Security Incidents from occurring in the future.

2.14.7 At New York Life's request, for any Security Incident in which New York Life Data is implicated, Supplier must retain and make available to New York Life complete, accurate, unredacted copies of all available system and network event log files on non-rewritable media beginning 72 hours prior to the Security Incident and running until 72 hours after the Security Incident was remediated. Supplier must store such media in a secure location until New York Life approves of its disposal. If New York Life requests the log files, Supplier must provide the files in a format that can be read by New York Life and may redact the data to remove information that does not pertain to New York Life, or to the products or services provided, so long as redaction does not compromise the log files.

2.14.8 Supplier must ensure proper forensic procedures, including chain of custody, are followed for the preservation and presentation of evidence to support potential legal action subject to the laws, regulations and procedures of the relevant jurisdiction, which may be brought against New York Life due to a Security Incident.

2.15 Identity Theft Red Flags

2.15.1 Supplier acknowledges that various United States Regulators have issued rules and guidelines (sometimes referred to as Red Flag Guidelines and Regulations, and including those implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003), requiring financial institutions and creditors to develop and implement policies and procedures to detect, prevent, and mitigate patterns, practices and specific forms of activity that indicate the possible existence of an actual or attempted theft or misappropriation of Personal Data. Supplier must comply with Applicable Laws and will assist New York Life in every reasonable manner in its efforts to fulfill its obligations under Applicable Laws.

2.15.2 Supplier must document, maintain and follow security practices and procedures to detect patterns, practices or activity that indicate theft or misappropriation of New York Life Data; Supplier must report to immediately report all incidences or suspicious activities to New York Life.

2.16 Payment Card Industry (PCI) Data Security Standard

2.16.1 If Supplier has access to or will collect, access, use, store, process, dispose of, or disclose credit, debit, or other payment cardholder information in the course of performance for New York Life, then Supplier must remain in full compliance with the Payment Card Industry Data Security Standard (PCI DSS) requirements, including any updates, at its sole cost and expense.

2.17 Audits and Verification

2.17.1 Supplier must cause annual audits under SSAE 18 (or any successor authoritative guidance for reporting on service organizations) for its general operations and under AT-101 or ISO/IEC 27001:2013 (or any successor information security standards), including substantive review of the effectiveness of Supplier's controls for all Scoped IT Assets. Supplier will also provide New York Life with copies of each report (e.g. SOC 1 Type II, SOC 2 Type II, SOC 3) Supplier receives in connection with such audits.

2.17.2 Supplier must permit New York Life to perform onsite security and remote desk based audits and reviews to verify Supplier's compliance with this Standard. Reviews may consist of security assessments requiring responses from Supplier or its Personnel, and visits to locations where (or from where) New York Life's Data may be stored, processed, administered or otherwise accessed, or review of all records, files and systems in Supplier's or its Personnel's possession relating to the purposes above. Additionally, in the event of a Security Incident, New York Life may perform immediate audits of the affected Scoped IT Assets.

2.17.3 Supplier must permit New York Life to perform onsite and remote desk-based audits and reviews to verify Supplier's compliance with this Standard. Reviews may consist of security questionnaires requiring responses from Supplier or its Personnel, visits to locations where (or from where) New York Life's Data may be stored, processed, administered or otherwise accessed, or review of all records and files in Supplier's or its Personnel's possession relating to the purposes above. Additionally, in the event of a Security Incident, New York Life may perform immediate audits of the affected Scoped IT Assets.

2.17.4 New York Life will detail all findings from the review in a written notice to Supplier. Supplier must work with New York Life to identify means for correcting the problems and addressing the concerns to New York Life's reasonable satisfaction.

2.17.5 Supplier must grant New York Life the right to distribute and use the findings of any review with any New York Life Affiliate, auditor or regulator as may be necessary to transact business with Supplier or to fulfill any New York Life compliance or information security Policy.

2.17.6 Supplier must permit representatives of New York Life, with prior notice and at reasonable times, to examine and verify compliance with Supplier's obligations with respect to the safeguarding and use of New York Life Data and Scoped IT Assets, and the detection, prevention, and mitigation of an actual or attempted theft or misappropriation of computing resources and New York Life Data.

2.18 Viruses and Disablement

2.18.1 Supplier must (1) prevent the introduction and proliferation of any Virus into Scoped IT Assets, and any other systems or resources used by Supplier to provide the services and products to New York Life, and (2) ensure, during the writing, execution and copying of software delivered in connection with the provision of services and products to New York

Life, that any such software is free from any Virus, by testing, prior to delivery, any such software and any media on which it is to be delivered with a current version of a leading anti-virus application.

2.18.2 Supplier must immediately notify New York Life of any event related to Virus activity present on Supplier Systems or other resources provided or used by Supplier. Supplier must notify New York Life on the status of potential events and impacts from the beginning of an event through closure.

2.19 Business Continuity, Disaster Recovery and Resiliency Plan

2.19.1 Supplier must have business continuity and disaster recovery plans ensuring operational resiliency that meets the needs of New York Life.

2.19.2 Supplier must ensure business continuity and disaster recovery plans receive management approval on an annual basis. All major updates that review people, process, and technology related mission critical deliverables must be incorporated on a semi-annual basis or sooner as warranted.

2.19.3 Supplier must conduct periodic Business Impact Analysis (BIA) and/or Risk Assessments designed to identify and prioritize critical business functions, processes and estimated impact of downtime in line with industry best practices.

2.19.4 Supplier must design and test the Disaster Recovery plan to ensure that it satisfies and complies with New York Life's Recovery Time Objective (RTO) requirements and in line with industry best practices.

2.19.5 Supplier must test all systems, business applications, and infrastructure at least annually to validate recovery capabilities, and must demonstrate successful remediation within 90 days or an exception must be filed.

2.19.6 Supplier must immediately notify New York Life of any event related to disruptions in the operational activity on Supplier product/service or other resources provided to New York Life. Supplier must notify New York Life on the status of potential events and impacts from the beginning of an event through closure.

3.0 Additional Hosted Solutions Requirements

In addition to the general requirements set forth in this Standard, Hosted Solutions providers must also be fully compliant with the following hosted solution security requirements. If there is a conflict between a general requirement and these hosted solution security requirements, Supplier will comply with the more stringent requirement.

3.1 Comprehensive Security Program & Practices

3.1.1 Supplier must ensure that safeguards are implemented in its environment (based on policies and procedures, business critical Assets and/or sensitive user data, and compliance with legal, statutory, and regulatory compliance obligations) to ensure that New York Life Data is properly segregated and only accessible by authorized users.

3.1.2 Supplier must ensure mutually agreed to terms are defined and documented for the methods, formats and protocols to be used for data/information exchange, interoperability, portability, usage, and processing.

3.1.3 Supplier must maintain an inventory of New York Life Data, and document data flows across servers, databases, and network infrastructure (including geographic locations of all infrastructure).

3.2 Network and Communication Security

3.2.1 Supplier must, when possible, keep information in session and avoid using web browser cookies, however, if web browser cookies cannot be avoided, ensure that web browser cookies containing New York Life Data or information that should not be altered outside of the Hosted Solution are encrypted using Approved Encryption (which Approved Encryption is independent from any transport encryption such as Secure Sockets Layer); all other cookies must be opaque.

3.2.2 Supplier must ensure IP address and location filtering are used to authenticate connections from specific locations and equipment. Adequate controls must be in place to prevent the connection of unauthorized devices to New York Life applications and data.

3.2.3 Supplier must use New York Life approved Application Programming Interfaces (APIs).

3.2.4 Supplier must, at the request of New York Life, restrict access to any component(s) of the networks, systems, services, and applications used to provide products/services to New York Life.

3.3 Infrastructure/Platforms/Services/Desktop/Operations Security

3.3.1 Supplier must provide New York Life with written security configuration guidelines that fully describe all relevant configuration options for relevant software and the implications for the overall security of the software. These guidelines must include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how all should be configured for optimal security. The default configuration for the software must be set at highest security level.

3.3.2 Supplier must have and administer a documented and approved key management process that addresses all phases of key lifecycle management, including but not limited to key creation, key use, key storage, key recovery, key revocation, and key destruction.

3.3.3 Supplier must ensure all New York Life Data can be exported in an industry-standard format upon request.

3.3.4 Supplier must define and document a mobile device security policy including the following specifications:

1. restricts Supplier Personnel access to New York Life Data on mobile devices;
2. mandates encryption of all New York Life Data stored on the device; and
3. requires the use of central mobile device management software (with remote wipe functionality, malware detection), and requires other security controls to protect New York Life Data.

3.4 Identity and Access Management

3.4.1 Supplier must make the following available on request for all New York Life identities used in any Hosted Solutions: ID, last login, roles assigned to the ID within the Hosted Solution (i.e., administrator, read-only, etc.), and which Hosted Solutions have been accessed using the ID.

3.4.2 Supplier must ensure hosted solutions are secured using a web-based single sign-on (SSO) method accepted and approved (in advance) by New York Life (currently SAML 2.0 identity federation standards where New York Life has the identity provider role).

3.4.3 Supplier must use New York Life approved non-SSO method in advance of deployment for New York Life. Non-SSO methods must, at a minimum, enforce a password policy meeting New York Life standards.

3.4.4 Supplier must review and recertify End User access capabilities at least semi-annually. For identified access violations, remediation Supplier must follow established user access policies and procedures.

3.5 Business Continuity, Disaster Recovery and Resiliency Plan

3.5.1 Supplier must ensure Business Continuity and/or Disaster Recovery plan includes processes and procedures for resuming operations promptly and not longer than 48 hours or sooner (as approved by New York Life) after the event.

3.5.2 Supplier must perform a Data Center Recovery Exercise at least annually or as required by State or Federal regulatory guidelines for all business areas. Any deviation from the Recovery Time Objective (RTO) approved by New York Life must demonstrate successful remediation within 90 days or an exception must be filed.

4.0 Additional Outsourced Delivery Center (ODC) Security Requirements

In addition to the requirements in Section 2, ODC Suppliers must be fully compliant with the following ODC Security requirements.

4.1 Comprehensive Security Program & Practices

4.1.1 Supplier must identify a named individual responsible for monitoring and reporting non-compliance with the New York Life requirements.

4.2 Supplier Personnel

4.2.1 Supplier will ensure that it provides security training to all Supplier Personnel who will be assigned to New York Life in advance of Supplier Personnel assignment start date. Security training will include, but not be limited to role-based security awareness, protection of information, security expectations per supplier policies and New York Life Supplier Security Standard. Supplier will maintain a record of all Supplier Personnel that have attended security training and will make this information available to New York Life upon request.

4.2.2 In addition to the requirements set forth in Section 2.2.7, Supplier must maintain a list of Supplier Personnel who are no longer assigned to New York Life and must provide that list to New York Life on a monthly basis.

4.3 Physical Security

4.3.1 Supplier must ensure all ODC technology infrastructure (e.g. servers & network equipment) is dedicated to New York Life; is caged and locked; is distinct and segregated from co-tenants, and is subject to a formal documented auditable process to ensure appropriate management of access.

4.3.2 Supplier will maintain an access register for all persons entering the ODC, which will include, but not be limited to, date, time, name, and reason.

4.3.3 Supplier must ensure all New York Life project activities are carried out in the dedicated area of the ODC segregated from co-tenants.

4.3.4 Supplier must ensure all entrances to the ODC are protected with physical security and additional PIN/access card-based system for restricted entry and exit. Supplier must ensure CCTV cameras cover ODC entry and exit zones with CCTV recordings, and entry and exit logs (for PIN/access card systems) maintained for at least 90 days.

4.3.5 Supplier must build opaque enclosures that block visibility from outside the ODC to prevent shoulder-surfing by unauthorized personnel.

4.3.6 Supplier must ensure only named Supplier Personnel assigned to New York Life are permitted to enter the ODC. All other persons (excepting only maintenance and

emergency workers such as police, firemen, emergency medical services and similar individuals) require express prior approval of New York Life before entering any New York Life dedicated areas.

4.3.7 Supplier must ensure that bags and personal devices are not brought into an ODC without express written authorization of New York Life. Unless prohibited by Applicable Laws, bags must be inspected both upon entering and exiting the ODC.

4.3.8 Use of any camera feature on all personal devices (or any other camera use) by Supplier Personnel is prohibited.

4.3.9 Supplier must enforce a clear desk policy in the ODC and must deploy document shredders (cross-cut, pulverizing, or equally secure) for destroying documents.

4.3.10 Supplier must ensure printers are kept out of the ODC and that printing capabilities from ODC IT infrastructure is disabled.

4.4 Network & Communications Security

4.4.1 Supplier must ensure that the entire telecommunications and data network for the ODC, including routers, switches, and firewalls, is physically segregated, including separate network equipment and cabling, from Supplier's Internet access demarcation point. Network infrastructure used for the ODC must not be shared with any co-tenants.

4.4.2 Supplier must ensure cables are concealed to prevent accidental or malicious interference and labelled to maintain segregation without drawing attention to the usage.

4.4.3 Supplier must ensure all unused ports are disabled.

4.4.4 Supplier must ensure guest wireless access is disabled inside the ODC.

4.4.5 Supplier must maintain a firewall rule recertification process. Unused or inactive rules should be reviewed and removed periodically.

4.4.6 Supplier must enable firewall logging for all types of traffic and monitor for any suspicious activity. Firewall logs must be available for review when requested.

4.4.7 Supplier must prohibit access to Supplier email, Instant Messaging (IM), or any other Collaboration/Messaging sites from within the ODC. Supplier must provide details of such tools to be disabled within the ODC.

4.5 Telephony

4.5.1 Supplier must secure all call control elements (PBX) against unauthorized access.

4.5.2 Supplier must ensure voice systems have proper controls that comply with voice recording.

4.5.3 Supplier must not provide Call Detail Records (CDR) to a third-party without prior written authorization from New York Life.

4.6 Infrastructure/Platforms/Services/Desktop/Operations Security

4.6.1 Supplier must ensure only a New York Life certified, secure desktop technology is deployed in the ODC.

4.6.2 Supplier must ensure only New York Life authorized software is installed on desktops in the ODC.

4.6.3 Supplier must ensure administrator-level privileges to Scoped IT Assets are authorized by New York Life, and must provide a list of all Supplier Personnel with administrator-level privileges to New York Life on a monthly basis.

4.6.4 Supplier must ensure that all Internet access to the ODC is routed via New York Life proxy servers.

4.6.5 Supplier must ensure Remote Access (from outside the ODC) is prohibited unless approved in advance and in writing by New York Life. Approvals must be maintained and made available for both Supplier and New York Life audits.

4.7 Audits and Verification

4.7.1 In addition to any audit provisions in Supplier's agreements with New York Life or in New York Life Policies, Supplier will allow New York Life to perform onsite audits and reviews on a semi-annual basis to verify Supplier's compliance with this Standard. Any exceptions to the standard must be approved by authorized New York Life personnel.

4.8 Business Continuity, Disaster Recovery and Resiliency Plan

4.8.1 Supplier must ensure business continuity plans are reviewed and approved by New York Life on a periodic basis or as requested.

4.8.2 Supplier must perform a worksite recovery and/or table top exercise that simulate real events that would disrupt operations to New York Life at least annually to ensure plans remain viable and executable.

5.0 Glossary

5.1 Access Control

Access Control means to ensure that access to Assets is authorized and restricted based on business and security requirements.

5.2 Accountability

Accountability means responsibility of an entity for its actions and decisions.

5.3 Applicable Laws

Applicable Laws means, as applicable to New York Life, Supplier, and Supplier's affiliates (directly and as a service provider to New York Life), or to the products/services provided by Supplier to New York Life, for all countries, all then-current national, federal, state, provincial or local: (A) laws (including common law), ordinances, regulations, and codes; (B) any then-current national, federal, state, provincial, or local law that relates to the confidentiality, security and protection of personal data, employee information, customer and client information, electronic data privacy, trans-border data flow, or data protection; (C) binding court orders, judgments, or decrees (including consent agreements); (D) orders, requirements, directives, policy, rule, decisions, judgments, interpretive letters, guidance and other official releases of any Regulator; and (E) all bribery, fraud, kickback, or similar anti-corruption laws including the U.K. Bribery Act and the U.S. Foreign Corrupt Practices Act.

5.4 Approved Encryption

Approved Encryption means the following standards, as well as any successor industry-accepted encryption method or algorithm that establishes more protective standards or protocols or any other encryption method or algorithm as may be required or requested by New York Life:

a) Encryption algorithms must be industry-accepted and in wide use, tested by multiple independent parties and meet the minimum key lengths defined below.
    1. For symmetric encryption, minimum standard key length of at least 256;
    2. For asymmetric encryption, a minimum standard key length of at least 2048;
    3. Elliptic Curve systems should have 224 or higher; or
    4. Hashing algorithms should be SHA2 or SHA256 or better.

b) Data transmission of any New York Life Data over public networks (including the Internet) or wireless networks (including cellular) must be encrypted as follows:
    1. Methods that are approved are SFTP, FTPS, HTTPS, TLS or FTP with PGP encryption (any changes by Supplier to the method or standard of transmission used must be approved in advance by New York Life).
    2. Data transmissions via email will be appropriately encrypted using Transport Layer Security (TLS) 1.2 or later or S/MIME, or another encryption method approved by New York Life's Information Security & Risk Team.
    3. Other methods are subject to New York Life Information Security & Risk Team's approval.

5.5 Availability

Availability means the accessibility and usability of information.

5.6 Confidentiality

Confidentiality means the privacy of data; ensures that information is not disclosed to unauthorized persons or processes. The primary methods for achieving confidentiality are authentication, authorization, and encryption.

5.7 End User

End User means, depending on the context, (A) Supplier Personnel, and/or (B) New York Life's directors, officers, employees, agents, auditors, consultants, suppliers, service providers, and contractors.

5.8 Hosted Solution

Hosted Solution means that the services provided by a Supplier to New York Life are hosted within, and/or managed from the Supplier's environment, including any related Software, applications, databases, websites, servers, Supplier Systems, and any IT Infrastructure component.

5.9 Integrity

Integrity means the consistency of data; ensures that an unauthorized person or system cannot inadvertently or intentionally alter data.

5.10 High Risk Transaction

A High Risk Transaction is a transaction or client inquiry that poses a high potential for financial or reputational loss to either New York Life or its clients if the transaction is unauthorized and may include:

a) Change of Contact Information

b) Bank Account Change

c) Beneficiary Change

d) Disbursement of any amount or asset (i.e. cash or securities)

e) Request for Policy/Account Number

f) Request for tax forms, account statements, and annual policy summaries

g) Ownership Changes

h) Account Closure Requests

5.11 Least Privilege

Least Privilege means a security practice, similar to need-to-know, that requires minimal access to all data, applications, systems and networks in a computing environment. End Users (including service or support accounts), applications and systems must be able to access only the information and resources that are necessary for its legitimate purpose.

5.12 Multi-Factor Authentication

Multi-Factor Authentication means provision of assurance that a claimed characteristic of an entity is correct through the verification of at least two of the following types of factors:

a) Something a person knows (Knowledge Factor) – This represents information of which only the legitimate user should have knowledge (e.g. a password). Often referred to as basic authentication.

b) Something the person has (Possession Factor) – This represents a physical object, which is not trivial to the duplicate, over which only the legitimate user has possession and control (e.g. hardware token physical access to a protected location, etc.).

c) Something a person is (Inherence Factor) – This is using unique physical traits of an individual such as iris or fingerprint, which cannot be duplicated on another individual.

5.13 New York Life

New York Life means (A) New York Life Insurance Company, (B) any entity that directly or indirectly controls, is controlled by, or is under common control with New York Life Insurance Company, and (C) its and their respective directors, officers, employees, agents, auditors, consultants, suppliers, service providers, and contractors (excluding Supplier and Supplier Personnel).

5.14 New York Life Data

New York Life Data means: (A) all data or information of New York Life as provided to or obtained by Supplier; (B) all derivative works of the same created by New York Life or Supplier; (C) all data and information resulting from use by Supplier or New York Life of Scoped IT Assets; and (D) any data or information derived from other New York Life Data, including through de-identification, data mining, analytics, aggregating, profiling, augmentation, or manipulation.

For the avoidance of doubt, New York Life Data also includes all tangible or intangible information and materials, whether owned by New York Life or by a third-party, and whether provided or disclosed to Supplier, Supplier's affiliates, or Supplier Personnel by New York Life (its affiliates or its or their respective personnel), or accessed, observed or otherwise obtained or generated by Supplier pursuant to any potential or actual business with New York Life, or otherwise involving Supplier's provision of services, software or products to New York Life, that satisfies at least one of the following criteria:

a) Information or materials related to New York Life's or its customers' business, trade secrets, customers (including identities, characteristics and activities), business plans, strategies, forecasts or forecast assumptions, operations, methods of doing business, records, finances, Assets, technology (including software, databases, data processing or communications networking systems), Policies, data or information or materials that reveal research, technology, practices, procedures, processes, methodologies, know how, or other systems or controls by which New York Life's products, services, applications and methods of operations or doing business are developed, conducted or operated, and all resulting or derivative information or materials;

b) Information or materials designated or identified as confidential by New York Life, whether by letter or by an appropriate proprietary stamp or legend, prior to or at the time the information or materials are disclosed by New York Life to Supplier;

c) Information disclosed orally or visually, or written or other form of tangible information or materials without an appropriate letter, proprietary stamp or legend, if it would be apparent to a reasonable person, familiar with the financial services industry, that the information or materials are of a confidential or proprietary nature;

d) Information that is or includes any data or information that, either individually or when combined with other information, could be used to distinguish or trace an individual's identity, including, by example, (1) personally identifying information that is explicitly defined as a regulated category of data under any data privacy or data protection laws applicable to New York Life; (2) non-public information, such as a national identification number, passport number, Social Security number; driver's license number, or any other government issued identification number, (3) Protected Health Information (as defined under the Health Insurance Portability and Privacy Act and its implementing regulations), and any other health or medical information, such as insurance information, medical prognosis, diagnosis information, genetic information, or biometric records; (4) insurance policy or financial information, such as a policy number, employee compensation, credit card number, or bank account number; (5) sensitive personal data, such as name, address, telephone number, date and place of birth, mother's maiden name, race, marital status, gender, information regarding an individual's education, criminal history, employment history or sexuality); or (6) any other information given protected status under any privacy law; or

e) Records, finances, Assets, technology (including software, data bases, data processing or communications networking systems), data or other information or materials produced by Supplier for New York Life under an agreement (unless the agreement expressly states that such are owned by, or the Confidential Information of, Supplier).

5.15 Outsourced Delivery Center (ODC)

Outsourced Delivery Center (ODC) means all or a portion of an on-shore, near-shore, or off-shore facility dedicated to New York Life, from or through which Supplier Personnel provide services to New York Life, or have access to Scoped IT Assets, New York Life Data (excluding public data), systems, hardware, or software.

5.16 ODC Supplier

ODC Supplier means a Supplier that provides services to New York Life via an Outsourced Delivery Center.

5.17 Risk-Based Authentication

Risk-Based Authentication means authentication that detects anomalies or changes in the normal use patterns of an Account and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

5.18 Scoped IT Asset

Scoped IT Asset means (A) Supplier Systems, and (B) New York Life Data.

5.19 Security Incident

Security Incident means any actual, alleged, or potential unauthorized access, disclosure, compromise or theft of a Scoped IT Asset.

5.20 Subcontractor

Subcontractor means a contractor, agent, service provider, or consultant, including a Supplier affiliate who is not a party to the applicable Order, who is directly or indirectly retained or used by Supplier. In such cases, the scope of New York Life's third-party risk assessment, due diligence, and ongoing monitoring requirements may be expanded to include the Subcontractor.

5.21 Supplier

Supplier means the counterparty to New York Life in a contractual relationship for the provision of goods, products, or services.

5.22 Supplier Personnel

Supplier Personnel means, whether stated directly or derived from context, Supplier's or its affiliates' directors, officers, employees, agents, auditors, consultants, suppliers, service providers, and contractors (excluding New York Life's personnel). Supplier Personnel also includes the directors, officers, employees, agents, auditors, consultants or other representatives of any Subcontractor.

5.23 Supplier Systems

Supplier Systems means the technology infrastructure, including all servers, telecommunications systems, networks, Internet connections, storage (including disk storage), software operating systems, and applications used by Supplier (or any Subcontractor) (1) in connection with the provision or delivery of products or services to New York Life, or (2) to store, process, or manage New York Life Data.

5.24 Virus

Virus means any computer code or any other procedures, routines or mechanisms designed to: (1) disrupt, disable, harm or impair in any way the Scoped IT Assets and their orderly operation based on the elapsing of a period of time, exceeding an authorized number of copies, or advancement to a particular date or any other measure (sometimes referred to as "time bombs", "time locks", or "drop dead" devices); (2) cause the Scoped IT Assets to damage or corrupt any of New York Life Data, storage media, programs, equipment or communications, or otherwise interfere with New York Life's operations; or (3) permit Supplier, its Personnel, its licensors, or any other third-party, without having secured the prior written consent of New York Life, to track or monitor New York Life's systems or to otherwise access New York Life's systems for any reason (sometimes referred to as "traps", "access codes" or "trap door" devices).

5.25 Vulnerability

Vulnerability means weakness of an Asset or control that can be exploited by a threat.