Supplier Security Standard

Effective Date: July 2024

Table of Contents

1.0 Introduction and Purpose

New York Life has developed this Supplier Security Standard to ensure Suppliers protect and maintain the Confidentiality, Integrity, and Availability of New York Life Data and Supplier Systems.

This Standard provides the minimum security requirements based on industry control standards (e.g., National Institute of Standards and Technology - NIST, Organization for Standardization – ISO, Service Organization Control 2 - SOC 2, etc.) that all Suppliers must adopt to ensure that New York Life Data is protected from loss, misappropriation, mishandling, alteration, or other damage.

Supplier's failure to meet this Standard may expose New York Life, its employees, customers, and business partners to risk, and may 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 New York Life Data to meet this Standard.

This Standard supplements the Agreement. If there are conflicts or inconsistencies among this Standard, the Agreement, or another New York Life policy or standard, New York Life expects Supplier to comply with the terms that provide the greatest level of protection for New York Life and its Data.

As used in this Standard, any capitalized terms have the meaning set forth in the Agreement or, if not defined in the Agreement, the meaning set forth in Section 4.0 (Glossary) of this Standard.

2.0 Supplier Security Requirements

2.1 Enterprise Risk Management

2.1.1 Supplier must adopt, implement, maintain, review, and adhere to a documented security program that is approved by management to protect the Confidentiality, Integrity, and Availability of supplier systems including those that provide services to clients such as New York Life.

2.1.2 Supplier must perform annual risk assessments to evaluate required access to client data (e.g., New York Life Data) or information systems, the identification of assets having access to or storing client data, the data classification associated with those assets, and the security controls in place to protect the client data (e.g., New York Life Data) . Supplier must update its security program based on its risk assessments.

2.2 Nth Party Management

2.2.1 Supplier must have a documented Nth Party Management Policy that is reviewed, maintained, approved by management, and communicated to employees and contractors on a periodic basis or upon material changes to systems, processes, changes to law/regulations, etc.

2.2.2 Supplier must adhere to a third party risk management program for the selection, oversight and risk assessment for Subcontractors.

2.3 Information Assurance

2.3.1 Supplier must perform information security control assessments on all Supplier Systems processing or storing client data (e.g., New York Life Data).

2.3.2 Supplier must track and maintain all records, data, and schedules that allow for the complete and accurate reconstruction of all financial transactions and all other information and systems needed to support normal operations. Financial transaction logs required to support normal operations and obligations must be retained for at least 5 years.

2.3.3 Fraud prevention controls and monitoring must be in place for high risk transactions as defined by client (e.g., New York Life) to prevent unauthorized access, such as to disbursement limits.

2.3.4 Supplier must ensure the portability of all client data (e.g., New York Life Data) in a mutually agreed upon format upon request by client.

2.4 Asset & Information Management

2.4.1 Supplier must develop, implement, maintain, review, and monitor ownership, inventory, return, and acceptable uses of assets transmitting, processing, or storing client data (e.g., New York Life Data).

2.4.2 Supplier must develop, implement, maintain, and monitor procedures and controls for the secure handling, transfer, destruction, and disposal of assets transmitting, processing, or storing client data (e.g., New York Life Data).

2.4.3 Supplier will destroy any retained client data (e.g., New York Life Data) as soon as its retention obligations have been met, unless a Hold Order is in place, and will provide a Certification of Destruction (COD) that addresses, at a minimum, method of deletion, volume of data, and date range.

2.4.4 Supplier must have a documented data protection policy that includes encryption (e.g., cryptographic algorithms, key length, end-of-life, etc.), key management (e.g., certificate lifecycle), and message integrity (e.g., authentication, hashing functions, Digital Signatures, etc.) requirements.

2.4.5 Supplier must have the ability to comply with clients' (e.g., New York Life) requests for Hold Orders, searches, and retrievals.

2.5 Human Resource Security

2.5.1 Supplier must perform appropriate background checks on personnel accessing client data (e.g., New York Life Data) Data.

2.5.2 Supplier must ensure that its security program (including its cyber security and privacy policies) is published, updated periodically and upon material change to Supplier Systems, processes, or Applicable Law. Policies should be approved by the Supplier's management and communicated to all Supplier Personnel.

2.5.3 Supplier must provide security awareness training to all Supplier Personnel accessing client data (e.g., New York Life Data) Data and maintain a record of such training.

2.5.4 Supplier must implement and execute processes to remove access within 48 hours and acquire assets with access to client data (e.g., New York Life Data) Data from departing or terminated Supplier Personnel.

2.6 Physical and Environmental Security

2.6.1 Supplier must have a documented physical security program that is maintained, reviewed, approved by Supplier management and is communicated to Supplier Personnel on a periodic basis.

2.6.2 Supplier must maintain physical security for all assets (e.g., servers, archive systems, laptop computers, removable media, mobile device, etc.) with access to client data (e.g., New York Life Data).

2.6.3 Supplier must limit access to and within its facilities based on the principle of Least Privilege with access recertification being performed on a periodic basis.

2.6.4 Supplier must monitor access to its facilities (e.g., CCTV, security guards). Facility CCTV and electronic badge system access logs must be retained in accordance with defined retention standards.

2.6.5 Supplier must maintain, monitor, and test environmental controls (e.g., temperature, humidity, fire suppression, continuous power) at all facilities with assets providing access to client data (e.g., New York Life Data).

2.7 IT Operations Management

2.7.1 Supplier must have a documented change management/change control policy or program that is maintained, reviewed, approved by management and is communicated to appropriate Supplier Personnel on a periodic basis.

2.7.2 Supplier must ensure that any changes to Supplier Production Systems (e.g., network, applications) are monitored and controlled via a documented formal change management procedure.

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

2.7.4 Supplier must test, review, and approve all changes to the Production environment prior to the change being made and evaluated for successful implementation following the change.

2.8 Access Control

2.8.1 Supplier must have a documented Access Control program that is maintained, reviewed, approved by management, and is communicated to Supplier Personnel on a periodic basis.

2.8.2 Supplier must have documented policies and implement controls to provide need-to-know access based on Least Privilege, allowing unique identification of individual user accounts.

2.8.3 Supplier must utilize a process to request, change, and remove Supplier Personnel access to client data (e.g., New York Life Data), ensuring segregation of duties throughout the process.

2.8.4 Supplier must have a documented Access Control policy covering all applicable Supplier Systems to include adequate authentication/authorization methods (e.g., AD/LDAP, single sign-on, OAUTH 2.0, ACF2, and home grown, etc.), password provisioning, complexity, resets, and thresholds for lockout attempts and inactivity lockouts.

2.8.5 Supplier must support SAML 2.0 at a minimum for web-hosted applications. For non-SSO, Supplier must support a New York Life approved method that, at a minimum, enforces a password policy that meets New York Life standards.

2.8.6 Supplier must use Multi-Factor Authentication to remotely access Supplier's network and systems that access, process, and store client data (e.g., New York Life Data).

2.8.7 Supplier must ensure shared accounts are not used to access client data (e.g., New York Life Data) and passwords and tokens are not shared.

2.8.8 Supplier must review access rights at least annually for access recertification.

2.9 Application Management

2.9.1 Supplier must have a documented and approved, Secure Software Development Life Cycle (SSDLC) for the purpose of defining, acquiring, developing, modifying, testing and implementing a Supplier System or software.

2.9.2 Supplier must validate developed software by performing design reviews and code scans using Secure Development best practices (e.g., OWASP).

2.9.3 Supplier must test and deploy application patches and security updates in accordance with defined standards.

2.9.4 Supplier must capture sufficient application data (e.g., retention, login attempts, changes to configuration settings) to support security incident investigations.

2.9.5 Supplier hosted software must be appropriately licensed.

2.9.6 Supplier must build application configuration to industry security standards (e.g., session timeout, inactivity timeout, etc.).

2.9.7 Supplier must not use client (e.g., New York Life) production Personal Data in non-production environments.

2.9.8 For hosted application services, Supplier must maintain an inventory and documented flows for client data (e.g., New York Life Data).

2.10 Cybersecurity Incident Management

2.10.1 Supplier must have documented, and approved by management, Cybersecurity Incident Management processes to detect, analyze, respond to, mitigate, and recover from threats and security incidents. Incidents should be documented from detection to resolution (e.g., prioritization, root cause analysis, preventative controls).

2.10.2 Supplier must periodically review and update its Cybersecurity Incident Management processes incorporating lessons learned.

2.10.3 Supplier must retain detailed Cybersecurity logs files for all activity on assets storing, processing, and transmitting client data (e.g., New York Life Data) for at least 3 years (e.g., session data including user ID, date, time, actions performed, failed authentication attempts, unauthorized access attempts, etc.).

2.10.4 Supplier must immediately notify and provide continued status to clients (e.g., New York Life) of any event that impacts the security, (confidentiality, integrity or availability) of the services provided to the client (e.g., New York Life), including any actual, alleged or suspected unauthorized or inadvertent access to, or disclosure of New York Life Data.

2.11 Operational Resiliency

2.11.1 Supplier must have documented Business Continuity and Disaster recovery plans ensuring operational resiliency for services being provided to clients (e.g., New York Life).

2.11.2 Supplier must ensure Business Continuity and Disaster Recovery plans are reviewed, updated, and approved at least annually or when material changes have occurred that impact services provided to clients (e.g., New York Life).

2.11.3 Supplier must conduct periodic Business Impact Analysis (BIA) and/or Risk Assessments designed to identify and prioritize critical business functions, processes, dependencies, and estimated Recovery Time Objective (RTO) for services provided to clients (e.g., New York Life).

2.11.4 Supplier must ensure its Business Continuity and Disaster Recovery plan includes processes and procedures for resuming operations promptly and within the contractually agreed upon recovery time regardless of loss (e.g., site, data, equipment, system, application, staff, subcontracted service).

2.11.5 Supplier must test its Business Continuity and Disaster Recovery plan periodically, accounting for the various conditions (e.g., loss of data, staff, equipment, site, system, application) that could affect services being delivered to clients (e.g., New York Life). Results of all testing must be documented.

2.11.6 Supplier must maintain all backup/archival media, containing client data (e.g., New York Life Data), in physically and environmentally secure storage areas owned, operated, or subcontracted by the Supplier.

2.12 Compliance Management

2.12.1 Supplier must have procedures to ensure compliance with applicable legislative, regulatory, or contractual requirements (e.g., identification of regulatory changes, records management, compliance reporting, auditing to procedures).

2.12.2 Supplier must provide code of conduct training on a periodic basis (e.g., information confidentiality, conflict of interest).

2.13 Endpoint Security

2.13.1 Supplier must follow documented device security configuration industry standards (e.g., device hardening, antivirus protection, malware protection, password protection, session timeout, inactivity timeout, etc.).

2.13.2 Supplier must test and deploy endpoint patches and security updates in accordance with defined standards and manufacturer recommendations.

2.13.3 Supplier must monitor, alert, and act on breaches and suspicious activity on endpoint devices (e.g., mobile phones, laptop and desktop computers) accessing client data (e.g., New York Life Data) Data.

2.13.4 Supplier must enable desktop/laptop security controls (e.g., Data Loss Protection (DLP), deny local administrator privileges, block peripheral devices – USB, CD drives) and encrypt local hard drives for endpoint devices with access to client (e.g., New York Life) Confidential data.

2.13.5 Supplier must prevent uploading and transmitting of client data (e.g., New York Life Data) to cloud storage services (e.g., Dropbox, Box.com, Google Drive) and prevent non-work email accounts to be accessible from company devices that have access to New York Life Confidential data.

2.13.6 Supplier must prohibit screen capture tools (e.g., Snipping Tool, print screen, screen recording, cameras) for devices with access to client (e.g., New York Life) Confidential data. In instances where Supplier cannot prohibit screen capture tools, Supplier will implement data loss controls to monitor for inappropriate use.

2.13.7 Supplier must enforce acceptable use and clean workspace policies (e.g., clear desk, locked screen when leaving desk, etc.).

2.13.8 Supplier must ensure New York Life Data is not stored on endpoint devices.

2.13.9 Where Supplier provided VDI is used to access the client (e.g., New York Life (NYL)) network, the supplier must prohibit screen capture, copying and pasting between guest and host, and the mapping, mounting and sharing of disk drives internally and externally. If the supplier's VDI is internet facing, Multi-Factor Authentication (MFA) must be required.

2.14 Network Security

2.14.1 Supplier must have a documented network security policy and architectural diagram that is maintained, reviewed, approved by management, and is communicated to the supplier's personnel on a periodic basis.

2.14.2 Supplier must implement security controls (e.g., Intrusion Prevention/Detection System (IPS/IDS)) to monitor and protect client (e.g., New York Life) Data over its internal and external network communications.

2.14.3 Supplier must configure network-related components of Supplier Systems (e.g., firewalls, network routers, switches, load balancers, domain name servers, mail servers, AWS, Azure, etc.) in accordance with its risk assessment and generally accepted information security standards.

2.14.4 Supplier must periodically review network-related components of Supplier Systems (e.g., firewalls, network routers, switches, load balancers, domain name servers, mail servers, AWS, Azure, etc.) configurations and rule sets to correct configuration drift and ensure rule sets allow only authorized services and ports that match the documented business justifications.

2.14.5 Supplier must test and deploy network patches and security updates in accordance with defined schedules and manufacturer recommendations.

2.14.6 Supplier must implement network segregation of Supplier Network (e.g., DMZ, internal, wireless, etc.) in accordance with their risk assessment and generally accepted information security standards.

2.14.7 Supplier must ensure Data Loss Protection (DLP) software is installed to block and alert on attempted external transfers of client data (e.g., New York Life Data) to scan email attachments, and block unauthorized traffic, etc.

2.15 Privacy Management

2.15.1 Supplier must have a documented and approved privacy program for the protection of Personal Data collected, accessed, transmitted, processed, disclosed, or retained on behalf of the client (e.g., New York Life).

2.15.2 Supplier must implement controls to protect the unauthorized disclosure of client (e.g., New York Life) provided Personal Data.

2.15.3 Supplier must immediately notify New York Life of any event that will impact the Confidentiality, Integrity or Availability of client (e.g., New York Life) provided Personal Data.

2.16 Artificial Intelligence (AI)

2.16.1 Supplier must have documented policies, processes, or procedures to oversee the design, development, deployment, testing, and monitoring of AI systems and their inventories.

2.16.2 Supplier must ensure decisions made or supported by AI systems are accurate and aligned with legal and regulatory requirements as needed.

2.16.3 Supplier must prevent unauthorized access and ensure the protection of client data (e.g., New York Life Data) utilized by AI systems.

2.17 Supply Chain Cybersecurity Risk

2.17.1 Suppliers must account for Subcontractor products or services in their security and operational resiliency policies and planning.

2.17.2 Suppliers must account for Subcontractor incidents in their Incident Management Policies or procedures.

2.18 Threat Management

2.18.1 Supplier must have a documented Threat Management program capturing security alerts from internal and external sources to identify and monitor for emerging security threats (e.g., vulnerabilities, ransomware, malware, DDoS) in their environment.

2.18.2 Supplier must have a documented Vulnerability Management policy or program designed to assess and maintain its security program. The policy should be approved by management, communicated to appropriate Supplier Personnel, and reviewed and updated on a periodic basis.

2.18.3 Supplier must periodically perform vulnerability scans and penetration tests against their internal and external network and application infrastructure accessing (e.g., process, store or transmit) client data (e.g., New York Life Data).

2.18.4 Supplier must prioritize and develop a remediation plan for all identified vulnerabilities within the Vulnerability Management program's remediation timelines consistent with the vulnerability's risk and industry standards (e.g., CVE).

2.19 Server Security

2.19.1 Supplier must build and update server configurations in alignment with industry security hardening standards. Server configurations must be periodically reviewed by Supplier for drift, and Supplier must perform regular patching for compliance with approved build images.

2.20 Cloud Services

2.20.1 Supplier must utilize cloud hosting providers that have been certified by an independent third party for compliance with domestic or international control standards (e.g., National Institute of Standards and Technology – NIST, Organization for Standardization – ISO).

2.20.2. Supplier must build virtual server hardened configurations in alignment with industry security standards. Server configurations must be, periodically reviewed server configuration for drift, and perform regular patching for compliance with approved build images.

2.20.3 Supplier must ensure backup data/image snapshots are stored in an environment with security controls commensurate with the production environment.

3.0 Appendix

Note: Without limiting the generality of the preceding sections, NYL has established the following minimum requirements and guidance based on industry control standards:

3.1 Supplier must ensure that all remote access to New York Life Data is performed utilizing the applicable NYL Approved Encryption.

3.2 Supplier must use Multi-Factor Authentication for any access to New York Life Data (including its accounts on Amazon Web Services (AWS), Microsoft Azure, and other cloud service providers) not originating within supplier networks or systems.

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

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

3.5 For dedicated and non-dedicated Service Delivery Centers (SDC), supplier must identify a named full-time Supplier employee responsible for monitoring and reporting non-compliance with the New York Life requirements.

3.6 Dedicated Service Delivery Center (SDC) Security Requirements include the requirements of 2.0 Supplier Security Requirements and the following:

3.6.1 Physical Security

(a) Supplier must ensure all SDC 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.

(b) Supplier must maintain an access register for all persons entering the SDC, which will include, but not be limited to, date, time, name, and purpose.

(c) Supplier must ensure all New York Life project activities are carried out in a secure and dedicated area of the SDC accessed only by Supplier Personnel dedicated to providing services to New York Life and fully segregated from co-tenants and unauthorized personnel.

(d) Supplier must ensure all entrances to the SDC are protected with physical security and additional PIN/access card-based system for restricted entry and exit. Supplier must ensure CCTV cameras cover SDC entry and exit zones with CCTV recordings for at least 90 days, and entry and exit logs (for PIN/access card systems) maintained for at least 3 Years.

(e) Supplier must build opaque enclosures that block visibility from outside the SDC to prevent shoulder-surfing by unauthorized personnel.

(f) Supplier must ensure only named Supplier Personnel assigned to New York Life are permitted to enter the SDC. All other persons (excepting only maintenance and emergency workers such as police, firemen, emergency medical services and similar individuals) require express prior written approval of New York Life before entering any New York Life dedicated areas.

(g) Supplier must ensure that bags and personal devices are not brought into an SDC without express written authorization of New York Life. Unless prohibited by Applicable Law, any permitted bags must be inspected both upon entering and exiting the SDC.

(h) Supplier must obtain written approval from New York Life before 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 Systems.

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

(j) Supplier must ensure printers are kept out of the SDC and that printing capabilities from Supplier Systems leveraged by the SDC IT infrastructure is disabled.

3.6.2 Network & Communications Security

(a) Supplier must ensure that the entire telecommunications and data network for the SDC, 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 SDC must not be shared with any co-tenants.

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

(c) Supplier must ensure all unused ports are disabled.

(d) Supplier must ensure guest wireless access is disabled inside the SDC.

(e) Supplier must maintain a firewall rule recertification process. Unused or inactive rules should be reviewed and removed at least annually.

(f) 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.

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

3.6.3 Telephony

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

(b) Supplier must ensure voice systems have proper controls that comply with voice recording.

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

3.6.4 Infrastructure/Platforms/Services/Desktop/Operations Security

(a) Supplier must ensure only a New York Life certified, secure desktop technology is deployed in the SDC.

(b) Supplier must ensure only New York Life authorized software is installed on desktops in the SDC.

(c) Supplier must ensure that all internet access to the SDC is routed via New York Life proxy servers.

(d) Supplier must ensure Remote Access (from outside the SDC) is prohibited unless approved in advance and in writing by New York Life. All such approvals must be maintained and made Available for both Supplier and New York Life audits.

(e) Supplier must ensure administrator-level privileges to Assets storing processing or transmitting NYL confidential data 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.

(f) Supplier must ensure business continuity plans are reviewed and approved in writing by New York Life on a periodic basis or as requested.

(g) 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.

4.0 Glossary

The following defined terms supplement Exhibit 1.1 (Definitions) of the Agreement under circumstances where a capitalized term in this Standard is not defined in Exhibit 1.1 (Definitions) of the Agreement.

4.1 **Access Control means** to ensure that access to Supplier Systems or to NYL Data is authorized and restricted by Supplier based on business and security requirements.

4.2 **Approved Encryption means** the following industry-accepted standards (e.g., NIST), 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:

4.2.1 Encryption algorithms must be industry-accepted and in wide use, tested by multiple independent parties and meet the minimum key lengths defined below.

(a) For symmetric encryption, minimum standard key length of at least 256 bits;
(b) For asymmetric encryption, a minimum standard key length of at least 2048 bits;
(c) Elliptic Curve systems should have 224-bit ECC or higher; or
(d) Hashing algorithms should be SHA2 or SHA256 or better.

4.2.2 Data transmission of any New York Life Data over public networks (including the Internet) or wireless networks (including cellular) must be encrypted as follows:

(a) Methods that are approved are SFTP, FTPS, HTTPS, Secure Shell (SSH) 2.0 or later, TLS 1.2 or later, FTP with PGP file encryption, and Virtual Private Network (VPN) (any changes by Supplier to the method or standard of transmission used must be approved in advance by New York Life).
(b) 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.
(c) Wireless networks must be encrypted using WiFi Protected Access 2 (WPA2) or later.
(d) Remote access to New York Life Data is performed over encrypted connections in alignment with current industry accepted standards (e.g., SSH, SCP, SSL-enabled web management interfaces, and VPN/VDI solutions).
(e) Other methods are subject to New York Life Information Security & Risk Team's approval.
(f) All Hardware Security Modules (HSM) must adhere to NIST FIPS 140-2 Security Requirements for Cryptographic Modules standard.

4.3 **Confidentiality generally 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. Confidentiality requirements are more specifically set forth in the Agreement.

4.4 **End User means**, depending on the context, (A) Supplier Personnel, and/or (B) New York Life Personnel.

4.5 **Hold Order(s) is** a notice issued in connection with litigation and regulatory matters and require the preservation of certain electronic and physical Records and non-records (documents).

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

4.7 **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.

4.8 **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:

4.8.1 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.

4.8.2 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.).

4.8.3 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.

4.9 **New York Life** has the same meaning as 'NYL' as set forth in the Agreement.

4.10 **New York Life Data means** New York Life's Confidential Information and NYL Materials (as each term is specified in the Agreement or, if not specified in the Agreement, as defined in New York Life's Supplemental Glossary for Supplier Security Standard).

4.11 **Personal Data means** 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 (A) information about or related to natural persons that is explicitly defined as a regulated category of data or given protected status under Applicable Law; (B) non-public information, such as a government-issued passport, Social Security, driver's license, or other identification number, (C) PHI and other health or medical information, such as insurance, medical, diagnosis, genetic, or biometric records or information; (D) financial and insurance information, such as employee compensation or a policy, credit card, or bank account number; or (E) 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).

4.12 **Service Delivery Center (SDC) means** all or a portion of an on-shore, near-shore, or off-shore facility, from or through which Supplier Personnel provide services to New York Life, or have access to NYL Systems, New York Life Data (excluding public data), systems, hardware, or software and which is solely dedicated to supporting NYL.

4.12.1 Non-Dedicated SDC means all or a portion of a facility that is not solely dedicated to performing New York Life services, and the technology infrastructure (e.g., firewalls, routers, etc.) may not be solely dedicated to New York Life.

4.12.2 Dedicated SDC means all or a portion of a facility that is solely dedicated to New York Life, where the SDC technology infrastructure (e.g., servers & network equipment) is dedicated to New York Life; is distinct and segregated from co-tenants and is subject to a formal documented auditable process to ensure appropriate management of access.

4.12.3 SDC Supplier means a Supplier that provides services to New York Life via a Service Delivery Center.

4.13 **Record(s) means** NYL Data that must be retained due to legal or regulatory requirements or because they capture significant business activity, regardless of the format (e.g., electronic or physical)

4.14 **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.

4.15 **Supplier Managed Device(s) are** endpoint devices that are managed by the Supplier including device configurations and security settings. Managed Devices include, but are not limited to laptops, desktops, tablets and mobile phones.

4.16 **Vulnerability means** weakness of Supplier Systems or controls that can be exploited by a threat.