EXHIBIT ___

Wolters Kluwer Global
Information Security Standards

Information Security Standards for WK Suppliers ("ISSWKS")

Document Number: GBS-STD-1203a
Document Version: 4.1
Last Revised: Dec 2024

Internal Use Only

Introduction

These Information Security Standards for Wolters Kluwer Suppliers ("**ISSWKS**") outline the logical and physical security requirements that Supplier shall maintain as part of the Services.

Part A: Definitions

Artificial Intelligence System or "AI System" means (i) a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments, or (ii) any other systems or services defined as artificial intelligence, machine learning, or the similar term under applicable law. AI System includes, but is not limited to, models and systems that can generate new text, images, video, audio, code, data, and other content based on natural language user queries and inputs.

End-User Device is any desktop or laptop, mobile device (e.g., cellular phone, smartphone, tablet), server and/or storage device that, (i) is involved in the performance of the Services, (ii) may be used to access a Network or an Environment, or (iii) may access or store WK Data.

Environment is any computing Environment, including but not limited to development, testing, staging, production and/or backup application, to which Supplier is provided access under an agreement or that is used to provide Services and contains WK Data.

Facilities means (i) any offices, data centers or all other locations (whether owned or managed by WK, a WK Affiliate, WK subcontractor, Supplier, Supplier Affiliate or Supplier subcontractor) from which WK Data, Environments or Networks may be accessed or (ii) any permanent or non-permanent location handling or storing WK Data or Information Systems.

Hosting Services is defined as any externally hosted technology offering for enabling convenient, on-demand Network access to a shared pool of configurable computing resources (e.g., Networks, servers, storage, applications and services).

Information Systems means all software, equipment and other technology that is (a) provided by WK or (b) provided by the user or by a third party and used in connection with the business of WK. This includes, without limitation, laptops, desktops, servers, mobile devices, email services, websites, networks, software, applications, operating systems, databases, data storage devices (including portable devices), security devices and other systems provided or maintained by WK.

Network means any WK network to which Supplier is provided access in connection with the performance of Services under the Agreement and/or any Supplier network that may access WK Data.

Personal Data means all information relating to an identified or identifiable natural person, plus any other data protected by Privacy Laws and processed in the context of the Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by

reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Privacy Laws means all laws, in any jurisdictions worldwide, that relate to (i) the confidentiality, processing, right to privacy, information security, protection, obligation to provide data breach notifications, transfer or trans-border data flow of Personal Data, or customer information, or (ii) electronic data privacy; whether such laws are in place as of the effective date of this DPA or come into effect during the term. Privacy Laws include but are not limited to EU GDPR, the CCPA and the UK GDPR.

Security Incident is any confirmed or reasonably suspected breach of Supplier's Network or Information Systems that has compromised or may compromise the confidentiality and integrity of WK Data, the availability of services to WK, or the security of WK Environments and its assets. This includes, but is not limited to, a breach of Supplier's security procedures, whether intentional or accidental.

WK Data shall mean, in or on any form, format or media (written, verbal, electronic or otherwise), and regardless of the manner through which it is obtained, furnished or made available (including, without limitation, through verbal exchanges or on-site visits) or the timing thereof (whether before or after the Effective Date of this Agreement), all data, analyses, summaries, reports, forms, files, records, documents and other information (a) that is related to WK, any of its Affiliates or any of their personnel, customers, vendors or other business partners, or otherwise furnished or made available by, through or on behalf of WK or its Affiliates, including any of the foregoing that is in WK's or any of its Affiliate's databases or otherwise in the possession of WK or any of its Affiliates on the Commencement Date or at any time from such date through the last day of the Term; (b) that may be received, computed, developed, generated, used, or stored by Supplier, or by any of Supplier's subcontractors, for WK or any of its Affiliates in the performance of Supplier's duties under this Agreement, including input materials and processed data; (c) prepared by or for the Supplier or any of its Representatives that are, in whole or in part, based on, reflecting, summarizing, derived from or incorporating anything encompassed by the foregoing clauses (a) or (b); (d) including this Agreement and the content hereof and any data relating to the performance or pricing of the Services; and (e) including all modifications, compilations and copies of any of the foregoing and (f) "Personal Data".

Part B: Personnel Security

B.1 Supplier must have a privacy and security awareness programs for all personnel, including third party subcontractors retained by Supplier, who will have access to WK Facilities, Networks, Information Systems, Environments and/or WK Data.

B.2 All Supplier personnel are required to agree, in writing, to abide by Supplier's privacy and security program(s), policies, procedures, standards, and processes.

B.3 Supplier must remove access to Facilities and Networks for Supplier personnel within 24 hours upon termination, including physical access to Facilities, as well as removal of accounts

for applications, systems and remote access capability.

B.4 Supplier's privacy and security awareness programs shall focus on topics relevant to the types of Services being delivered to WK and that are specific to the role.

B.5 Supplier shall provide (for the avoidance of doubt, at Supplier's own cost) all developers and QA personnel a minimum of 8 hours of application security training per calendar year, through eLearning or in-person trainings.

B.6 Supplier must ensure Supplier personnel complete the privacy and security awareness program training no later than two months after beginning of employment with Supplier and annually thereafter.

B.7 Upon request, Supplier shall provide written confirmation for each calendar year of compliance with these training requirements.

Part C: Supplier Security Procedures and Risk Assessments

C.1 Supplier must provide WK with a designated contact representative for matters related to information security, privacy and corporate security.

C.2 Supplier agrees to conduct comprehensive security and risk assessments on an annual basis either internally, by the Supplier's qualified security personnel, or by an independent third-party audit firm specializing in security assessments and report detailed results to WK upon request. Findings shall be evaluated for possible corrective actions.

Part D: Audit and Compliance Checks

D.1 The allocation and use of privileges shall be restricted to Supplier personnel with a legitimate need to know or need to have such privileges in order to perform the Services. Such privileges shall be controlled by an individual responsible for granting privileges to appropriate Supplier personnel. If Supplier personnel will have access to WK-managed Facilities, Networks or Environments, Supplier must maintain a complete list of all personnel with permission to such access including their geographic location. Supplier must periodically review the list and promptly notify WK of updates required.

D.2 Within 30 days of WK's request, Supplier must certify to WK in writing its compliance with the requirements of this ISSWKS, any other security and privacy requirements or measures that have been agreed with WK and provide written responses to any questions that WK submits to the Supplier about its security practices. This can include questions submitted to the Supplier by WK or a request by WK to the Supplier to provide an independent audit report, such as an ISO 27001 certification, SOC 2 Type 2 attestation report or similar report.

D.3 WK may perform security audits at WK's expense, to confirm compliance with this ISSWKS and industry best practices. Supplier cannot charge WK (i.e. time spent on audit) and must ensure that WK has direct access and rights to audit subcontractors at supplier's site or supplier's subcontractor's site upon reasonable notice, or alternatively provide independent attestation, such as per AICPA, ISO, CSA or other standards.

D.4 Supplier must promptly correct all security issues identified in an onsite security assessment

performed by WK or a third party working under the direction of WK. Supplier must promptly correct any security issues identified by Supplier or WK pursuant to the above reviews.

Part E: Security Incident and Reporting

E.1 Supplier must email WK at the address below to report any Security Incident within 24 hours. WK maintains a Security Operations Center (SOC) that is staffed 24/7/365 days a year.

Email: ThirdPartyIncident@wolterskluwer.com.

E.2 Supplier must take appropriate steps to immediately address any Security Incident as defined in Part A and must cooperate with WK with respect to the investigation of such Security Incident. Supplier must promptly provide WK updates and results of the investigation and follow WK's instructions concerning the security of WK's Networks, Information Systems and other WK Data.

E.3 Supplier may not make or permit any statements concerning any such Security Incident to any third party, including news media, without the explicit written authorization of WK, except that Supplier may contact law enforcement or other authorities where required by law.

E.4 Supplier must meet all legal requirements of breach notification and any additional requirements agreed to between the parties.

E.5 Unless the Security Incident is caused by WK, (a) where notice by Supplier is legally required, Supplier will provide credit monitoring to all affected individuals, at Supplier's expense, with input from WK; and (b) otherwise, Supplier will provide notice and credit monitoring, at Supplier's expense, only upon WK's request.

Part F: Information Security Controls

F.1 Information Security Policy and Organization of Information Security

F.1.1 Supplier must maintain a formal written information security program which includes policies, standards and procedures for the administration of information security throughout the organization that are consistent with common information security standards and frameworks such as NIST, ISO 27001, COBIT or a comparable information security standard or framework. The information security policy must communicate management's commitment to information protection and the responsibilities of personnel for the protection of WK Data. Policies, standards and security procedures should be reviewed, updated and approved by Supplier firm's management at least annually.

F.1.2 Supplier must have a security function with clearly defined information protection roles, responsibilities and accountability. Upon request, the Supplier must provide WK contact information of the person(s) WK may contact in relation to any information security issues or Security Incidents and ensure that any changes are promptly communicated to WK's liaison, project manager or other individual identified in the Agreement.

F.2 Operations management

Supplier must apply the following controls to any Networks and/or End-User Devices that may access WK Networks, Environments and/or access or store WK Data.

F.2.1 Supplier may not maintain or store any WK Data except as necessary for the performance of Services under the Agreement.

F.2.2 Supplier must store all WK Data in a secure location, ensuring that appropriate physical security controls (including facility and environmental controls) are in place to prevent unauthorized physical access to Facilities or damage to WK Data. If Supplier uses vendors for transporting or storing backup media, Supplier must assess all such vendors in order to verify the confidentiality, integrity and availability of backup media and must make documentation detailing such information available to WK upon request. All back-up media that leaves Supplier's facility must be encrypted using 256-bit or stronger encryption.

F.2.3 Supplier may not store WK Data on any mobile device or removable media (such as external disks, USB memory storage, smartphone, cell phone or backup media) unless required for the performance of Services. If under the rare exception that WK Data needs to be stored on removable media, it must first be approved by WK and then must be encrypted using 256-bit or stronger encryption. Supplier must require that all personnel use strong passwords or biometrics on all of their mobile devices, and the mobile devices must be configured to fully wipe all data automatically after no more than ten incorrect password attempts and remotely wiped if it is reported lost or stolen.

The Supplier must securely wipe all Environments and WK Data from electronic media and End-User Devices in a manner that ensures that the WK Data is not able to be accessed or read. Such deletion must take place upon WK's request or as soon as such storage is no longer required for the performance of Services, including without limitation upon the completion of the Services. If applicable Environments are hosted externally by Supplier, Supplier will cause the hosting provider to sanitize the environment in a manner equivalent to those requirements included in section F.2.4.If electronic media will be redeployed, the Supplier must use a sanitation process that ensures data is securely wiped. It must destroy boot partitions, file pointers and user data, as well as prevent all data from being reconstructed and read.

To securely wipe WK Data, Supplier must follow NIST.SP.800-88.

F.2.4 Supplier may retain one copy of the data for so long as required by law, as long as:

- The Supplier notifies WK in writing that the copy will be retained and the reason for such retention;
- The copy is kept in encrypted format;
- The copy is not used or accessed for any other purpose; and
- A date for secure removal has been documented and WK is notified upon destruction.

F.2.5 If the Supplier is providing Services that involve the receipt of electronic media from WK that stores WK Data, upon the completion of the use of the media for the Services, the Supplier must either sanitize the media in accordance with Section F.2.4 or return the electronic media to WK by a carrier providing package tracking and delivery confirmations.

F.2.6 The Supplier must securely dispose of all documents and all defective electronic media containing WK Data by cross-shredding or using a secure disposal bin designated for disposal of

confidential materials. These secure disposal methods must include appropriate processes (such as a certificate of destruction) and auditable practices that ensure that the documents or defective electronic media cannot be re-created, accessed or read.

F.2.7 The Supplier must not retain any record of WK Data, either electronic or paper, for more than five business days after processing unless otherwise agreed to in writing by WK or as required by applicable law or regulation. (As used in this paragraph, “record” includes any WK Data, in any format, and on any media, including originals and copies. “Processing” includes any use of WK Data where the information is not required to be stored by the Supplier). In the event that any WK Data is lost or destroyed while subject to the Supplier’s possession, access or control, the Supplier must notify WK within the timeframe specified in this ISSWKS (see E.1), and at the request of WK, and at the Supplier’s own expense, use best efforts to reconstruct such information, data and/or files as soon as feasible.

F.2.8 Upon termination of the Agreement, or at any time upon request by WK, the Supplier must return all WK Information Systems regardless of format (including, but not limited to documents, papers, photographs, copies, computers, and electronic media) to WK within five business days unless otherwise agreed upon in the Agreement.

F.3 Patching and Vulnerability Management

F.3.1 The Supplier must apply the appropriate operating system, database, and application security patches promptly, when issued by the manufacturer, on all End-User Devices. The Supplier must configure End-User Devices to automatically receive operating system, database and application security patches when issued, unless such patches may interfere with the operation of the End-User Device, in which case patches must be tested promptly and applied upon successful test completion. If a security patch cannot be applied because it interferes with the operation of the End-User Device, the Supplier must implement effective risk mitigating controls.

F.3.2 Supplier must have a formal vulnerability management program in place that includes periodic system and application scans, annual penetration tests and vulnerability remediations, based on risks.

F.4 Anti-virus

F.4.1 The Supplier must use end-point security protection and/or anti-virus software to prevent, detect and remove malicious programs (malware), such as viruses, worms, spyware and Trojans, from systems. If the software employs known file-based malware signatures and mechanisms, both automated signature updates and disk scans across all systems commonly affected by malicious software (particularly personal End-User Devices and servers) must be performed at least weekly.

F.4.2 The Supplier must enforce automatic virus and malicious code scanning checks on all electronic attachments and files that are sent to or received from external sources. Email attachments that are infected with known malicious code must be removed prior to delivery.

F.5 Operations and Change Management

F.5.1 The Supplier must have security and acceptance criteria defined for new and upgraded End-User Devices and Networks that can access or store WK Data. The criteria must address testing (and mitigation) of operating system, middleware, database and application security vulnerabilities, to help ensure that adequate security controls exist for those particular Environments.

F.5.2 The Supplier must maintain documented change management procedures that provide a consistent approach for controlling and identifying changes for all systems and Network infrastructure that may be used to provide services and/or that may access or store WK Data.

F.5.3 The Supplier must define roles and responsibilities in a manner that allows for appropriate segregation of duties, to prevent fraud and potential malicious or accidental misuse of Supplier systems, applications and Networks that are used to provide Services to WK.

F.5.4 The Supplier must ensure that the use of utility programs that are capable of overriding system and application controls (e.g. booting up from peripheral devices) are restricted and controlled.

F.5.5 The Supplier must change all vendor supplied default passwords before the system is live in a production Environment.

F 5.6 Supplier must not use production data in Environments used for development, testing or other non-production purposes

F.6 Remote Access and Exchange of Information

F.6.1 When accessing Environments over the Internet, the Supplier may use only encrypted Network traffic via industry Standard Virtual Private Network (VPN), SSL VPN or equivalent technology. Any other methods of remote access connectivity need to be approved in writing by WK Information Security, prior to connecting to the Environment, unless otherwise specified in the Agreement.

F.6.2 The Supplier may only transmit WK Data over the Internet using current versions of encryption mechanisms (e.g., HTTPS, SSL, SFTP, TLS, etc.).

F.6.3 If email is the primary method of exchanging WK Data, the Supplier must use encrypted email. WK provides services for protecting email between WK mail gateways and Supplier mail gateways using Transport Layer Security (TLS).

F.6.4 The Supplier must implement Multi-factor authentication (MFA) for access to systems storing WK Data.

F.7 Access control

F.7.1 The term “user” in this section includes Supplier personnel with access to systems that access or store WK Data, including but not limited to privileged accounts for support purposes.

F.7.2 Supplier personnel must terminate their Network connection or access when no longer required for the performance of the Services.

F.7.3 The Supplier must implement controls that lock an account after five invalid attempts

have been made to login.

F.7.4 The Supplier must implement user account management policies and procedures to support the secure creation, amendment and deletion of user accounts in the Supplier's Environment. These procedures must include processes for monitoring redundant accounts and for ensuring that information owners properly authorize all user account requests.

F.7.5 The Supplier must ensure that user accounts for access to Environments that contain WK Data are attributable to single individuals (e.g. unique identifier, passwords). The Supplier must not use generic or shared user accounts. The Supplier must instruct its personnel not to share user account credentials.

F.7.6 The Supplier must enable operating system access controls that restrict access to End-User Devices and Environments that process or store WK Data. These controls must verify the identity of users, record the source location (IP address) of each successful and failed system access attempt, and restrict the connection times of users. The Supplier must maintain system access logs for a period of at least three months and make the logs available to WK upon request.

F.7.7 Login must occur for all users of an information system used to store, process and/or transmit WK Data, including re-authentication when accessing said data.

F.7.8 The Supplier must require users to re-authenticate after a period of inactivity not exceeding 30 minutes. Activity includes any input to the endpoint (e.g. mouse, keyboard, touch screen).

F.8 Passwords

F.8.1 The Supplier must maintain and enforce the following password requirements for any Supplier Environment or End-User Device used to access WK Networks, Environments and WK Data. For the avoidance of doubt, the term "user" in this section includes Supplier personnel with access to systems that access or store WK Data, including but not limited to privileged access accounts for support purposes.

a) The Supplier must issue new user accounts and passwords to users in a secure manner that ensures their confidentiality.

b) The Supplier must force users to change their passwords at the first logon and no less frequently than every 90 days thereafter.

c) The Supplier must distribute passwords separately from account information.

d) Password Reuse –maintain a record of previously used passwords and prevent the re-use of the previous five passwords.

e) The Supplier must enforce strong password practices that include a minimum password length based on industry best practice of at least eight characters, password complexity includes:

- a mix of alpha numeric characters
- Upper case letters (A, B, C, ….Z)

- Lower case letters (a, b, c, ….z)
- Numbers (0,1, 2, …9)
- Non-alphanumeric (“special characters”) such as punctuation symbols, and

F.8.2 All passwords must be encrypted during transmission and authentication for applications. Systems must not allow connections on unencrypted channels or services.

F.9 Supplier’s Network Infrastructure

F.9.1 Supplier Networks used to access WK Data must have security controls that can detect attacks by making use of firewalls, intrusion detection/prevention systems (IDS/IPS) and other Network infrastructure (e.g. routers, load balancers). Networks must have continuous monitoring. The Supplier must record and log all Network security related activities (e.g. security events, errors) with logs maintained for a period of at least three months. All logs must be made available to WK upon request.

F.9.2 In shared Environments, WK Data must be logically segregated (and physically separated, where technically feasible) from that of other customers and must have access controls to prevent WK Data from being accessible or visible by personnel not directly assigned to WK accounts.

F.9.3 The Supplier must ensure that a perimeter network (i.e., DMZ) is implemented such that internal information systems and applications that are used to store, process and/or transmit WK Data and that are accessible from the Internet are protected.

F.9.4 Remote access and host security must implement group-based access controls to limit access to Network resources in the Supplier Network.

F.9.5 The Supplier must develop and implement Network use cases to monitor, detect and protect against malicious Network behavior including but not limited to Web Application Firewalls (WAFs), configured in protect mode, and designed with rule-sets that filter or block undesired traffic intended for web-based services and applications related to the Agreement.

F.10 Information Security and Regulatory Compliance

F.10.1 The Supplier may access, use and process WK Data only on behalf of WK and only for the purposes specified in the Supplier’s Agreement with WK, in compliance with these Standards and such further instructions as WK may provide regarding the processing of such information.

F.10.2 The Supplier may not use WK Environments or WK Data for development or testing of any system other than the WK system specified in the Agreement, unless such additional use is specified in a separate Agreement.

F.10.3 The Supplier must use Data Loss Prevention (DLP) capabilities to monitor and protect WK Data in the Supplier Network. The Supplier must establish measures to limit information leakage (covert channels) to unapproved Hosting Services (e.g. data sharing services).

F.10.4 The Supplier must inform WK promptly if the Supplier has reason to believe that legislation applicable to the Supplier (or changes in legislation applicable to the Supplier)

prevents it from fulfilling the obligations relating to treatment of WK Data and/or the Supplier's Agreement with WK.

F.10.5 If the Services provided by the Supplier involve access to and handling of PHI as defined by the U.S. Health Insurance Portability and Accounting Act (HIPAA), the Supplier must implement the applicable safeguards and processes for the access to and handling of PHI that are specified in the HIPAA Privacy and Security Rules: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/

F.10.6 If the Services involve access to credit and/or debit card information, the Supplier must ensure that it is in compliance with the current version of the Payment Card Industry (PCI) Data Security Standards (DSS) for the duration of the Services provided to WK. On request, the Supplier must provide WK with a current PCI Attestation of Compliance performed by a third-party PCI qualified security assessor or if unavailable, an Internal Security Assessor accredited by the PCI Council.

F.10.7 To the extent permitted by law, the Supplier must notify WK promptly and act only upon WK's instruction concerning:

a) Any request for disclosure of WK Data by law enforcement or other governmental authority

b) Any request by law enforcement or other governmental authority for information concerning the processing of WK Data in connection with this Agreement

c) Any request received directly from an individual concerning his/her WK Data

F.10.8 The WK entity whose Personal Data is accessed pursuant to an Agreement may enforce the terms of this ISSWKS as permitted or required by applicable law.

F.10.9 The Supplier must not store, transfer or grant access to WK Data to any country with United States Government sanctions. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals. An up-to-date list of countries with U.S. sanctions can be located at:

http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

F.11 Hosting Services

F.11.1 This ISSWKS applies to any use of Hosting Services to store, process, or transmit WK Data..

F11.2 The Supplier must use physical restrictions (e.g., IP whitelisting) to limit access to privileged user self-service functionality.

F11.3. The Supplier must formally train any Supplier personnel with responsibilities for implementing or managing Supplier's use of Hosting Services about secure implementation and use of those services.

F.11.4 The Supplier must receive WK approval for any proposed material changes to the approved use of an external Hosting Services before they are executed. (Material changes are anything beyond routine maintenance e.g. patches)

F.12 Information Systems Acquisition, Development, and Maintenance

F12.1 The Supplier must incorporate information security requirements into its processes and procedures for the selection, development and implementation of applications, products and services.

F12.2 The Supplier must have a secure build procedure for all systems where WK Data is stored, processed and/or transmitted.

F12.3 The Supplier's secure build procedure must include tools to support automated configuration checking of the security and standard build settings at the time of production deployment and over the lifetime of the build.

F.13 Online Security Threats

F.13.1 The Supplier must have controls in place to protect against online security threats consistent with Open Web Application Security Project (OWASP) (e.g., cross-site scripting, SQL injection). A complete list of updated online security threats can be located at https://www.owasp.org/

F.13.2 The Supplier must use input validation for all Internet and intranet applications.

F.14 Cryptographic Controls

F.14.1 The following table describes encryption requirements for the Supplier. For transmissions involving WK Data, the Supplier must use encryption for application-to-application or server-to-server communications. When WK Data is stored or transmitted by a Supplier-hosted application, the Supplier is responsible for compliance according to the following table:

Function / Data	Encryption in Transmission	Encrypt in Storage
WK Data	All Environments	All Environments
Remote Access	All Environments	N/A

F.14.2 External Individual Email: The Supplier must use transport encryption (e.g., gateway-to-gateway encryption via Transport Layer Security (TLS)) when emailing individual messages containing WK Data between WK and the Supplier, when the Supplier is not permitted to use WK-approved end-to-end encryption software or tools per regulation and/or the Supplier's policy.

F.14.3 External Parties: When WK Data is provided by the Supplier to an external party (subcontractor), that external party must either meet the requirements of these encryption requirements or provide comparable controls validated by an Information Security assessment and accepted by the Supplier. (Such information must be encrypted in transit to and from the Sub-contractor when sent electronically.)

F.14.4 Supplier must encrypt any voice data stored containing WK Data.

F.14.5 Wireless networks: The Supplier must encrypt their wireless networks with industry standard encryption algorithms.

F.15 Additional Supplier Security Agreements

F.15.1 Additional security requirements may be specified in Supplier's Agreement or individual statement of work.

F.16 Third Party Service Providers

F.16.1 WK must grant prior written permission before the Supplier provides WK Data or access to a WK network to a third-party service provider providing Services to WK under the Agreement.

F.16.2 Supplier shall be responsible for ensuring third party service providers' adherence with security terms substantially similar to those of this ISSWKS. Supplier must ensure that contractual obligations with the third-party service provider include applicable and enforceable security terms.

F.16.3 Supplier must conduct periodic risk assessments of third-party service providers and make the assessments available to WK upon request.

F.17 Information System Management

a. Inventory of Information Systems

F.17.1 The Supplier must maintain an inventory of all applications and Information Systems under its control that are used to store, process and/or transmit WK Data and make the inventory available to WK upon request.

F.17.2 If the Supplier uses functional usernames (e.g., service accounts) on production or Continuity of Business (CoB) information systems, the Supplier must maintain an inventory(s) of the usernames, capturing the key attributes.

b. Protection of Information Systems

F.17.3 The Supplier is responsible for protecting all WK Data under its control.

F.17.4 All functional usernames on production/CoB information systems where WK Data resides must only be created if an owner is designated.

c. Access and Acceptable Use of Information Systems

F.17.5 The Supplier must ensure accountability of its users' activity in a manner consistent with industry best practice.

Part G: Network/Environment Access

This section sets forth the terms applicable to the Supplier's access to and use of WK's Network, Environment and information technology resources. It is not applicable to the Supplier-provided SaaS environments (Software as a Service).

G.1 The Supplier may only use the Network connection for approved business purposes. The use of the Network connection for unapproved purposes, including but not limited to personal use or gain is strictly prohibited.

G.2 The Supplier may only use access methods which have been approved by WK.

G.3 Only authorized Supplier personnel may access WK Networks and Environments to perform the Services specified in an Agreement. The Supplier must ensure that only their employees or contractors that are doing work on behalf of WK and approved by WK in advance, have access to the Network connection or any WK owned equipment.

G.4 The Supplier must be solely responsible for ensuring its employees or contractors are not security risks. Upon request from WK, the third party must provide WK with any information reasonably necessary for WK to evaluate security issues.

G.5 The Supplier must promptly inform WK in writing of any relevant personnel changes. This includes the rotation and resignation of personnel so that WK can disable their usernames and remove / change passwords in order to secure its resources.

G.6 As part of the annual service agreement review, the Supplier must provide WK with an up to date list of their personnel who have access to the Network connection or any WK owned equipment, upon request.

G.7 The Supplier must ensure at all times that all End-User Devices used by them to connect to the WK Network have reputable up to date anti-virus software and the appropriate security patches installed.

G.8 The Supplier must ensure all unnecessary services and protocols are disabled in accordance with NIST SP 800-123. http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

G.9 Under no circumstance, encrypted or otherwise, should WK Data be stored by the Supplier on removable media including a mobile device or USB memory keys/sticks.

G.10 The Supplier must ensure that all End-User Devices used by them to connect to the WK Network, are used in such a way that information belonging to WK is not displayed to unauthorized individuals or the public.

G.11 The Supplier must ensure that all their End-User Devices connected to the WK Network are not connected to any other Network at the same time, with the exception of Networks that are under the complete control of the Supplier.

G.12 When the Supplier is connected to the WK Network, they should not leave their End-User Device unattended.

G.13 The Supplier must ensure that when they are connected to the WK Network their activity does not disrupt or interfere with other non-related Network activity.

G.14 All Supplier End-User Devices used to connect to the WK Network must be made available for inspection upon request.

G.15 The Supplier Network connection will by default be granted read / execute privileges only. All requests for increased privileges must be submitted in writing to WK where they will be considered on a case-by-case basis.

G.16 The Supplier must obtain the written consent of WK before implementing any updates or amendments to the WK Network, information systems, applications or equipment. All approved updates and amendments implemented by the Supplier must be made in line with the WK's change management policies and procedures.

G.17 The Supplier must ensure all software is scanned and cleared of all viruses and other forms of malicious software before it is installed on any WK Network or in any WK Environment. The third party will be held responsible for all disruptions and damage caused to the WK Network or Environment which is traced back to infected software installed by the Supplier.

G.18 To the extent permitted by law, WK reserves the right to monitor Supplier's access to and use of Networks, Facilities and any End-User Devices accessing Networks. WK reserves the right to revoke the Supplier access privileges at any time, for any reason, or no reason at all.

Part H: International Transmission of WK Data

H.1 Backup and other processes at locations in countries other than where WK Data was originally provided to Supplier will not receive, maintain, process, or otherwise access such WK Data except with the prior written consent of WK.

Part I: Business Continuity and Disaster Recovery

I.1 Supplier must maintain a Disaster Recovery (DR) program and maintain a documented organizational Business Continuity Plan (BCP) for systems that process or store WK Data. The program and plans must be designed to ensure the Supplier can continue to function through operational interruption and continue to provide services as specified in its agreement with WK. Supplier will provide WK written summaries of its DR program and BCP upon request.

I.2 Alternate sites and infrastructure should be appropriately secured and periodically tested to support the business continuity in case of disaster. Upon request by WK, the Supplier will provide confirmation of tests performed, including identified gaps and remediation actions or plans.

I.3 Supplier must promptly notify and report the potential impact to WK Data when either of the plans are executed.

Part J: Information Backup

J.1 Supplier must ensure Information Systems, computers and Software involved in the performance of the Services provided to WK are backed up to online and/or offline storage. Backups must be tested in accordance with operational backup standards.

J.2 Backup media leaving Supplier's facility must be protected against unauthorized access, misuse or corruption during transportation. WK Data stored on backup media must be encrypted using 256-bit encryption.

Part K: Artificial Intelligence

K.1 Supplier will implement processes and procedures to ensure that it does not use or cause to be used any WK Data in any manner to create, train or improve (directly or indirectly) any AI System unless WK expressly consents to such use in writing.

K.2 The Supplier shall retain WK Data only for the necessary duration, promptly deleting it upon completion or termination of the agreement including any “inputs” into the AI System and any corresponding generated “output”.

K.3 Subcontracting involving WK Data is strictly prohibited without the prior written consent of WK (which consent may be provided in the Agreement). Any approved subcontractors must adhere to the same stringent data protection and security standards outlined in the Agreement.

K.4 The Supplier commits to providing clear explanations for how the AI System works prioritizing model outputs, utilizing interpretable model architectures and algorithms, and furnishing comprehensive documentation on the entire AI System and any model training process.

K.5 The Supplier undertakes to fortify AI Systems against adversarial attacks by employing robust content anomaly detection, implementing continuous monitoring, and incorporating adversarial resistance measures, including adversarial training and real-time detection mechanisms throughout the lifecycle of such systems.

K.6 Supplier agrees to implement processes and procedure to ensure that AI Systems have been and will be designed, developed and deployed using a responsible artificial intelligence assurance framework substantially similar to the NIST AI Risk Management Framework and WK’s AI Principles each as amended from time to time.