INFORMATION SECURITY REQUIREMENTS FOR KODAK DATA

These Information Security Requirements (the "Requirements) for Kodak Data are mandatory for every Kodak Supplier. These Requirements allow Kodak and Supplier to demonstrate compliance with applicable privacy, security and data protection laws. Supplier agrees that it shall comply with the terms of this Exhibit with respect to all Personal Information and Confidential Information collected, used, transmitted or maintained for Kodak and its affiliates. Capitalized terms used herein but not defined below have the meanings given to them in the Kodak Data Processing Agreement and/or the services agreement(s) between the parties.

1. Definitions.

(a) "**Kodak Data"** means collectively all Personal Information processed by Supplier for Kodak and Kodak Confidential Information.

(b) **"Kodak Systems**" means all technology solutions and equipment, all associated or interconnected network equipment, routers, embedded software, and communication lines, and all components of any information system or equipment owned or operated by, or operated on behalf of, Kodak.

(c) **"Internal Control Report"** means a Type II Service Organizational Control (SOC) report (based on the SSAE 18 or ISAE 3402 model) or any successor report thereto or an ISO 27001 Certification Report (if applicable).

(d) "**Security Policies**" means the Supplier's internal written information security policies which document the Supplier's approach for protecting the confidentiality, integrity and availability of Kodak Data, computers, and network systems, consistent with established industry standards and best practices and mandating compliance with applicable laws and regulations.

(e) "**Security Procedures"** means statements of the step-by-step actions taken to achieve and maintain compliance with Security Policies. Security Procedures must include (without limitation) security controls, processes, procedures, and technologies for administrative, physical, technical and organization security domains, cybersecurity, and incident response.

(f) "**Security Technical Controls**" means any specific hardware, software or administrative mechanisms necessary to enforce Security Policies and Security Procedures, including (without limitation) technologies, methodologies, implementation procedures, and other detailed factors or other processes to be used to implement security requirements relevant to specific groups, individuals, or technologies.

(g) **"Subprocessor"** means any third party (including an affiliate of Supplier) that provides any services to Supplier and that may have access (including inadvertent access) to any unencrypted Kodak Personal Information.

2. Internal Control Assessment and Reports.

(a) Unless an exception is provided in the applicable Statement of Work, Supplier shall conduct at its own expense annual independent annual assessments of controls relevant to the security, availability, processing, integrity, confidentiality and/or privacy of the products, applications and/or platforms use to process Kodak Data under the Agreement. These assessments shall be conducted by a independent, reputable third party organization o a recognized auditing standard such as SSAE18.

(b) Supplier shall undergo an annual network security assessment by an independent third-party organization that specializes in providing this type of security assessment. Assessments must include, but are not limited to, vulnerability scans quarterly, penetration tests annually, and assessment upon major changes to the infrastructure or applications.

(c) Once per year, Supplier shall provide Kodak with copies of the applicable Internal Control Reports. Kodak understand that the responses and Internal Control Reports contain Confidential Information of the Supplier, and it shall not disclose the Internal Controls Reports other than to its auditors and advisors in connection with verifying Supplier's compliance with Kodak's security and privacy program requirements. If any internal control assessment determines that a material deficiency exists at a Supplier facility, Supplier shall, upon learning of the determination, notify Kodak in writing regarding the material deficiency and, at Supplier's expense, remediate the deficiency.

3. <u>Business Continuity Planning.</u>

Supplier shall have implemented and documented appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services in a timely manner after a disruptive event. Supplier will regularly test and monitor the effectiveness of its business continuity and disaster recovered plans. At appropriate intervals or as otherwise requested by Kodak, Supplier will provide Kodak with a detailed summary of its written business continuity and disaster recovery plans.

4. <u>Information Security Obligations</u>

(a) Supplier shall have implemented and documented appropriate administrative, technical and physical measures to protect Kodak Data against accidental or unlawful destruction, alteration, unauthorized disclosure or access. Supplier will regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures. Supplier will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Kodak Data, and ensure that these risks are addressed. Supplier will review and (if appropriate) update its Security Policies, Procedures, and Technical Controls at least annually.

(b) Supplier shall strictly enforce and comply with its Security Policies, Security Procedures, and Security Technical Controls. Supplier shall have implemented a formal security awareness program for all personnel that includes training on proper use of security measures and on the importance of security for Kodak Data. Personnel will be appropriately monitored for compliance with the Security Policies, Security Procedures, and Security Technical Controls. Supplier shall have a defined disciplinary procedure to address violations of security policies or procedures by personnel, which must include the possibility of termination

(c) Supplier's security program shall include periodic security risk assessments and regular testing as needed for it and for Kodak to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for timely remediation. Testing and monitoring must include (without limitation):

i. Quarterly reporting on vulnerability status & patch management
ii. Development and adherence to OLAs for vuln closure
iii. Annual penetration testing
iv. Monthly DAST scanning
v. Maintenance of SOC2
vi. Quarterly SCA/SBoM scans and reports

Supplier will provide results of the testing and monitoring with Kodak upon request.

(d) Supplier shall strictly enforce and implement:

i. Physical protection mechanisms for all information assets and information technology to ensure such assets and technology are stored and protected in appropriate data centers; appropriate facility entry controls are in place to limit physical access to systems that store or process Kodak Data; processes to ensure access to facilities is monitored is and restricted on a "need to know" basis; and controls to

physically secure all Kodak Data and to properly destroy Kodak Data when it is no longer needed.

ii. Logical access controls, including appropriate mechanisms for user authentication and authorization in accordance with a "need to know" policy; controls to enforce rigorous access restrictions for remote users, contractors and service providers; timely and accurate administration of user account and authentication management; processes to ensure assignment of unique IDs to each person with computer access; processes to ensure Supplier-supplied defaults for passwords and security parameters are changed and appropriately managed ongoing; mechanisms to track all access to Kodak Data by unique ID; the use of passwords and other secure authentication credentials; mechanisms to encrypt or hash all passwords; and processes to immediately revoke accesses of inactive accounts or terminated/transferred users.

iii. A security architecture that reasonably assures delivery of reasonable and appropriate security, including documented and enforced technology configuration standards; processes to encrypt Kodak Data in transmission, including travel across public networks and wireless, and, in storage including backups, archives, laptops and portable devices where technically feasible; processes to ensure regular testing of security systems and processes; a system of effective firewall(s) and intrusion detection technologies necessary to protect Kodak Data; and database and application layer design processes that ensure web site applications are designed to protect the Kodak Data that is collect, processed, and transmitted through such systems.

iv. Mechanisms to keep security patches current; processes to monitory, analyze, and respond to security alerts; appropriate network security design elements that provide for segregation of data; use and regularly update anti-virus software; and processes to regularly verify the integrity of installed software.

v. Appropriate administrative security controls to reasonably manage risks associated with Supplier's workforce (such as appropriate background checks, training, and oversight) and Supplier's third party processors.

vi. Password management controls such that the passwords that are associated with access to the Kodak Data must contain at least eight (8) characters that must be alpha numeric and must include both upper and lower case and include special characters. Account lockout will occur after five (5) failed access attempts. Passwords must be encrypted when transmitted between information systems, network devices and applications.

vii. If mobile devices are used in the delivery of services to Kodak, devices must be managed using centralized device management software that has the capability to remotely lock and wipe lost/stolen devices.

viii. For systems or applications associated with the access, processing, storage, communication and/or transmission of Kodak Data, Supplier will generate audit logs for actual or attempted incidents of unauthorized use, access, disclosure, theft or data manipulation. These logs must be maintained for a minimum period of ninety (90) days and stored log files on a centralized logging server. Log events must at least contain the information "Who" (users or systems that produced the event), "What" (event details including the event's success or failure index), "When" (time stamping) and "Where" (origin, destination, or object of the event). Supplier must review these logs in accordance with defined Security Procedures, and maintain adequate records of the review of such audit logs for purposes of audit or other applicable legal or regulatory requirements. If Suppliers review of the audit logs reveals reasonable evidence of any unauthorized use, access, disclosure, theft, manipulation, reproduction and/or security breach involving Kodak Data, Supplier must notify Kodak of the incident via email to ww-ciso-mail@kodak.com within twenty-four (24) hours. Audit logs will be provided to Kodak upon request.

(e) If any Supplier personnel will perform the Services onsite at a Kodak facility or who have access to Kodak Systems:

i. As permitted by applicable law, Supplier will cause such personnel to submit to background investigations by Kodak or its designee, including criminal history and providing evidence of the person's right to work in the particular location where the Services are being performed. Supplier will obtain written consents from such personnel as may be necessary to conduct such investigations and provide these to Kodak upon request.

ii. Supplier will comply with (and will cause all Supplier personnel to comply with) all Kodak policies and procedures governing access to the Kodak facilities and Kodak Systems for security, change control and system documentation. Supplier shall be granted limited access to the Kodak Systems for the exclusive purpose of undertaking the transactions and services provided for in this Agreement. Supplier represents and warrants that (A) neither Supplier nor any Supplier personnel will gain or attempt to gain access to any Personal Information, Confidential Information or other Kodak Systems other than to the extent necessary to render specific Services and (B) Supplier will not allow any Supplier personnel to gain access to the Kodak Systems who does not reasonably require such access.

iii. Supplier is responsible for protecting the authentication method of all Supplier personnel to the Kodak Systems and preventing any misuse of the ID and access method provided by Kodak to Supplier. Supplier hereby agrees to terminate the access of Supplier personnel promptly upon the conclusion of completion of such Supplier personnel's portion of the services under this Agreement.

(f) During the Term, Supplier shall not modify or amend the Security Policies, Security Procedures, or Security Technical Controls in a manner that makes such policies, procedures, controls, or practices less stringent. However, Supplier may amend the Security Policies, Security Procedures, or Security Technical Controls, manner that makes such policies, procedures, controls, or practices more stringent and/or more vigilant in protecting the security of the Kodak Data.

(g) Supplier specifically represents and warrants that, during the Term of the Agreement, it shall:

vii. store all Kodak Data on servers located in those countries disclosed to Kodak in writing (such as on Annex 1 to the Kodak Data Processing Agreement or in the applicable Statement of Work) which must be equipped with state of the art security mechanisms and controls to prevent unauthorized penetration or interception of the Kodak Data; and

viii. maintain separate and secure back-ups of all Kodak Data and conduct daily back-ups on those servers.

(h) Upon termination or expiration of the Agreement, (and at any other time, upon request), at Kodak's direction, Supplier will either (i) return the Kodak Data (and all media containing copies of the Information) to Kodak, or (ii) purge, delete and destroy the Kodak Data in accordance with industry standards instructions for secure destruction.

5. <u>Security Audits</u>.

(a) Upon request, Supplier shall provide Kodak with information about the Supplier's information security program. All such information is Confidential Information of Supplier.

(b) Upon reasonable advance written notice, Kodak shall have the right to perform: (1) a security audit of Supplier and/or its subcontractors, including as necessary to verify the integrity of Kodak Data and examine the systems that process, store, support and transmit that data and (2) an audit to examine Supplier's performance of the Services and conformance to the terms of this Agreement. If Kodak elects, the audit pursuant to the previous sentence may be performed by two (2) separate Kodak audit groups (i.e., one Kodak audit group performing the security portion of the audit, and another Kodak audit group performing

the Services performance portion of the audit). The audit procedures described in this Section also shall be utilized by Kodak, for Kodak's reviews of Supplier's business continuation and disaster recovery plans and business resiliency assessments.

All audits will be performed during Supplier's reasonable business hours, which shall be carried out by Kodak (or by a qualified independent auditor) in a mutually-agreeable manner (designed to validate Supplier's controls against an established industry standard such as ISO 27001) no more than ten (10) day after any such request.

If Kodak's ability to conduct onsite audits is limited by the nature of Supplier's hosting relationships, Supplier (or its Subprocessor) will submit its data processing facilities for audit at least annually, which shall be carried out by an independent auditor approved by Kodak in a manner designed to validate the entity's controls against an established security standard, such as ISO 27002. If any such audit reveals material gaps or weaknesses in the security program, Kodak shall be entitled to terminate Supplier's Processing of Personal Information until such issues are resolved.

(c) If Kodak performs a security audit pursuant to this Section and finds (based on a reasonable security risk assessment adhering to industry standard practices) that corrective action is warranted as a result of the audit, Kodak shall provide written notice to Supplier, including the audit details, documenting the alleged security failure with respect to Supplier and/or its subcontractors. Upon receipt, Supplier shall provide (at no additional charge) remedies acceptable to the Parties, to correct the audit failure (including, if applicable, ensuring that its subcontractors remedy such failure). If the remedy fails to satisfy the audit requirements, and no mutually acceptable solution is agreed upon by the Parties, then (A) Supplier shall be in material breach of the Agreement, (B) Kodak may elect, in its sole discretion, to terminate the Agreement (or the applicable Services affected by the security risk), and (C) if Kodak does terminate, Supplier shall refund to Kodak all pre-paid monies with respect to the terminated Services, if any, on an unused pro-rata basis; provided however, that for clarification, this item (C) applies only to pre-paid monies for Services not yet provided to Kodak and does not apply to Supplier's charges for already-provided Services.

(d) Supplier shall also cooperate with any audits conducted by any regulatory agency that has authority over Kodak as needed to comply with applicable law.

(e) Notwithstanding the previous language in this Section, in the event of a suspected or actual security or confidentiality breach, affecting Kodak's information or data, Kodak reserves the right to audit Supplier and/or its subcontractors performing Services for Kodak at any time following such breach to: (A) verify the integrity of Kodak's information or data and/or (B) examine the systems that process, store, support and transmit such Kodak information or data. At no charge to Kodak, Supplier will provide to such auditors and representatives such assistance as they reasonably require, and Supplier shall also reimburse Kodak for the reasonable cost of any such audit performed pursuant to this Section.