CLOUD AND SUPPORT SECURITY ADDENDUM TO THE
INFORMATICA LICENSE AND SERVICES AGREEMENT AND/OR DATA PROCESSING AGREEMENT

This Exhibit identifies security policies and commitments of Informatica for its Cloud Services and Support Services. Additional security features of each Cloud Service may be described in the Informatica Product Description Schedule or Cloud Description Schedule, as applicable. Informatica's privacy policy (which applies to the information collected about Customer's employees and contractors) is separate from this Exhibit and is available for reference at https://www.informatica.com/privacy-policy.html.

Informatica may update this Exhibit from time to time to document changes in security policies for the Cloud Services and/or the Support Services, in accordance with Change Management below. Informatica will, upon request no more than once per year, certify to its compliance with this Exhibit.

Solely for the purpose of this Exhibit, the definition of Customer Data is expanded to include any data that Customer submits to Informatica for analysis pursuant to the Support Services it requests.

Security Management System

Informatica has a risk-based, third-party-audited Information Security Management System ("ISMS") designed to enable Support Services to be delivered in a secure manner and designed to protect Cloud Services and related Informatica systems from threats and data loss. This Exhibit describes the controls of the ISMS as of the Effective Date of the Exhibit. Informatica regularly assesses and makes improvements to the ISMS with reference to changing security threats, regulatory requirements and industry standards.

Risk Assessment

Informatica conducts, or retains independent third parties to conduct, information security risk assessments at least annually and whenever there is a material change in Informatica's business or technology practices that may impact the privacy, confidentiality, security, integrity, or availability of Maintained Customer Data (as defined below). The risk assessment includes identifying reasonably foreseeable internal and external risks to privacy, confidentiality, security, integrity, or availability; assessing the likelihood of, and potential damage that can be caused by, identified risks; assessing the adequacy of personnel training concerning the ISMS; updating the ISMS to limit and mitigate identified risks as appropriate and to address material changes in relevant technology, business practices, and personal information practices and regulations; and assessing whether the ISMS is operating in a manner reasonably calculated to prevent and mitigate unauthorized access to or disclosures of Maintained Customer Data ("Security Incidents").

Standards

Informatica aligns its ISMS to the ISO27001 standard, and controls defined in the ISO 27002 standard are included in Informatica's associated policies and procedures. For select Cloud Services, Informatica annually receives third party audits for compliance with AICPA SOC 2 Type 2, SOC 3, and the U.S. Health Insurance Portability and Accountability Act ("HIPAA"), including as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"). The most recent certifications and/or audit summary letters, including an SSAE No. 18 report, are available upon Customer request under NDA. The most recent SOC 3 report is available upon request and is also available publicly on the Informatica Trust Center website at https://www.informatica.com/trust-center.html.

Data Processing and Storage

Processing and storage requirements for Customer Data on computer systems owned or licensed by Informatica or its suppliers for the Cloud Service or Support Service ("Informatica Systems") are determined by the type of Informatica Cloud Service or Support Service subscribed by Customer. Customer has sole responsibility for selecting a Cloud Service, and designing a system of which the Cloud Service is a part, that complies with laws and regulations applicable to Customer's use.

Type I Cloud Services, consisting of Informatica Intelligent Cloud Service, Informatica Cloud Service, Informatica Cloud Data Integration, and their variants, depend on a Customer-managed installation of a high function runtime version of Informatica's data processing execution component ("the Informatica Cloud Secure Agent") that moves data among sources, local systems, and targets. Type I Cloud Services therefore do not process or store Customer Data on Informatica Systems, provided that Type I Cloud Services may include an optional data preview display feature and/or optional support for Salesforce outbound messaging, which transiently send Customer Data to, but do not store Customer Data on, Informatica Systems. Type I Cloud Services may store on Informatica Systems metadata relevant to operation and data processing of the Informatica Cloud Secure Agent managed by the Customer. There are three categories of metadata that may be stored by Type I Cloud Services on Informatica Systems: Runtime Metadata, Organizational and User Security Metadata, and Design Metadata ("Metadata"). Runtime Metadata contain agent definition data and other information crucial for runtime activities, like connection and schedule data and activity logs. Organizational and User Security Metadata describe the structure of the organization, define users and groups and their permissions, privileges, access credentials, and license information, and track audit logs. Design Metadata define integration tasks and processes, including data sync, data replication, mappings and templates, task flows, process definitions, and connectors. Certain Informatica Cloud Services may use de-identified Design Metadata to generate design suggestions for Customer and other customers, subject to giving Customer notice and an opportunity to opt out. Informatica Systems that support Type I Cloud Services except legacy Informatica Cloud Service, and Informatica's operation thereof, undergo annual third-party audits for compliance with AICPA SOC 2 Type 2, SOC 3, and HIPAA/HITECH as referenced in the "Standards" section above.

Type II Cloud Services, consisting of Informatica Cloud API Manager, Informatica Cloud Application Integration, Informatica Cloud B2B Gateway, Informatica Cloud Data Wizard, Informatica Cloud Integration Hub, Informatica Data Quality Radar, Informatica Discovery IQ, Informatica MDM Cloud Edition, Informatica Operational Insights, Product 360 Cloud Edition, an Informatica Cloud Secure Agent for a Type I Cloud Service if hosted by Informatica at Customer's request, Informatica Cloud Real Time, Informatica Axon Data Governance Cloud Edition, and their variants, may transiently or persistently store Customer Data on Informatica Systems ("Maintained Customer Data"). Type II Cloud Services may store Metadata as described above on the same Informatica Systems that support Type I Cloud Services and may depend on a Customer-managed installation of the Informatica Cloud Secure Agent. Informatica will not use or disclose Maintained Customer Data for any purpose other than that of performing its obligations in connection with the Agreement. Informatica Systems that support Type II Cloud Services except Informatica Axon Data Governance Cloud Edition and legacy Informatica Cloud Real Time, and Informatica's operation thereof, undergo annual third-party audits for compliance with AICPA SOC 2 Type 2, SOC 3, and HIPAA/HITECH as referenced in the "Standards" section above.

Type III Cloud Services, consisting of Informatica "Data-as-a-Service" products and their variants, may transiently store Maintained Customer Data that are phone numbers, addresses, emails, or other applicable communication data processed by the Type III Cloud Services. Storage by Informatica Systems does not exceed the time necessary to process the data and make the results available for access by Customer. Informatica Systems that support Type III Cloud Services that process phone numbers and emails, and Informatica's operation thereof, undergo annual third-party audits for compliance with AICPA SOC 2 Type 2 and HIPAA/HITECH as referenced in the "Standards" section above.

Support Services

Support Services may require Informatica to receive Customer Data such as a detailed description of Customer's environment, a copy of Customer's repository, or a sample of the Customer's data. Customer will transmit such Customer Data via secure FTP site or physical media, and Informatica will store such Customer Data solely at Informatica Support Services facilities solely for the duration of the applicable Support Services investigation in accordance with the section titled Disposition of Data below. Support Services do not require Informatica to receive personal data and Informatica discourages uploading of any personal data. Customer must notify Informatica immediately in the event it mistakenly uploads personal data to ensure deletion from the system.

Support Services interactions between Informatica personnel and Customer through virtual meetings may be recorded.

By joining a virtual meeting session, Customer consents to recording and to Informatica's remote access to Customer's computer systems for provision on Support Services. Such access may allow Informatica to control, modify, or alter certain elements of Customer's computer systems. Customer is responsible for notifying Informatica personnel prior to exposure or possible exposure of personally identifiable information during virtual meeting sessions and for redirecting Informatica personnel and/or halting the session to avoid exposure.

Security – Overview

Informatica uses reasonable methods designed to safeguard Maintained Customer Data from unauthorized access, use, and loss including physical, technical, and administrative safeguards. Maintained Customer Data from different customers are segregated logically and/or physically. Informatica may use additional measures to enhance security beyond those listed below.

Security – Physical Security

Physical access to Informatica locations holding Informatica Systems have limited access points, which are governed by card or biometric access devices and monitored by surveillance cameras. Access to servers, network ports, wireless access points, routers, firewalls, or any physical computing equipment involved with data hosting is physically restricted.

Security – Access

Informatica's ISMS limits its access to Informatica Systems to authorized Informatica personnel. Access to Maintained Customer Data is authorized in accordance with individual role-based segregation of duties. Upon Customer's written request, Informatica will promptly identify in writing all Informatica personnel who have been granted access to the Maintained Customer Data as of the date of the request. Access authorizations for Informatica personnel are reviewed at least semi-annually and rescinded promptly upon change of roles or separation from Informatica. Informatica maintains logs of access by Informatica personnel.

Security – Authentication

All Cloud Services are accessible to Customers through interfaces requiring authentication. Type I and II Cloud Services include optional support for two factor authentication for user access.

Security – Encryption

Type I and II Cloud Services use TLS certificates with 2048/256-bit keys, SSH, and IPsec protocols for data transmission and remote access over public networks, and AES encryption for transmission and for protecting the database containing Customer Data or Metadata. Type III Cloud Services use encryption for all Web-enabled transactions that require user authentication or transfer of Customer Data. This is accomplished using one of the following methods: (a) TLS v1.2, (b) Secure Shell (SSH), (c) Secure File transfer protocol (SFTP), or (d) Virtual Private Network (VPN).

Informatica implements an encryption key management process. Encryption/decryption keys are managed independently of the native operating system access control system; stored with reasonable protections; protected during transmission or distribution, changed at or before they reach the end of their cryptoperiod; and retired if Informatica becomes aware that their integrity has been compromised. With the exception of one-time use password communication, all user passwords are encrypted with cryptography in transit and at rest on Informatica Systems. Valid user identifier and password combinations are encrypted via TLS while in transit.

Security – Harmful Code and Patches

Informatica Systems implement and maintain software designed to detect and prevent malicious code that may perform unauthorized functions or permit unauthorized access to any Informatica System, including computer viruses,

Trojan horses, worms, and time bombs. All critical and high vendor security patches are applied within thirty (30) days of release date. All medium rated security patches are applied within ninety (90) days of release date.

Security – Architecture

Informatica Systems accessible to the Internet are protected with server hardening, patch management, and incident management. Informatica Systems accessible to the Internet are protected with application firewalls in a DMZ architecture, with back-end systems such as databases further protected by a second set of application firewalls. Firewall and router rules are default-deny and reviewed for unnecessary services and IP address exposures at least once per six months.

Security – Product Development

Informatica implements Security as a Design Principle. The lifecycle of cloud product development, from secure application development training, application and code reviews, source code scans, vulnerability scans, penetration tests, responsible disclosure program, and other controls are implemented continuously to reduce the probability and/or impact of application vulnerabilities. All critical and high application security patches are applied within thirty (30) days of confirmation. All medium rated security patches are applied within ninety (90) days of confirmation date.

User Access Logs

Informatica maintains access logs to the Cloud Services including date, time, and User identifier. Informatica can provide Customer the access logs as required to comply with governing law to assist in forensic analysis if there is a suspicion of inappropriate access. Access logs will be maintained in a secure area for a minimum of ninety (90) days during the Term and destroyed in accordance with Disposition of Data below. Passwords are not logged under any circumstances.

Customer Security Controls

Certain Cloud Services include configurable security controls as indicated in the corresponding Documentation, including unique user identifiers to help ensure that activities can be attributed to the responsible individual, controls to revoke access and/or lock out a user after multiple failed login attempts, password length controls, termination of a session after a period of inactivity, and geographical and/or chronological restrictions on access.

Employees and Contractors

Informatica personnel that operate or support Cloud Services receive annual education on the importance of security, confidentiality, and privacy of Maintained Customer Data, Informatica policies and associated data security practices, and the risks to Informatica and its customers associated with Security Incidents. Informatica implements measures designed to ensure that its personnel are sufficiently trained, qualified, and experienced to be able to fulfill their functions under the ISMS and any other functions that might reasonably be expected to be carried out by the personnel responsible for safeguarding Maintained Customer Data.

Incident Management

Informatica cloud operations personnel receive regular training on standard operational procedures and tactics to minimize the impact of production cloud incidents. Such incidents are classified according to severity of impact, with high-severity incidents triggering root cause analysis and reviews to identify areas for long-term improvement.

Change Management

Informatica plans to enhance and maintain the Cloud Services and Support Services during the Term, including but not limited to changes in response to relevant technology and systems, unauthorized access to Maintained Customer Data, and the discovery of material privacy or security vulnerabilities. Security controls, procedures, policies and features may change or be added but will deliver a level of security protection that is not materially lower than that provided as of the Effective Date.

Informatica maintains a change management process with separation of duties and appropriate approvals required for modification to Informatica Systems, including patch management for the Cloud Services. Informatica uses risk- based criteria with remediation objectives for critical and high vulnerabilities.

Business Continuity and Disaster Recovery

Any facility housing Informatica Systems is designed to withstand adverse weather and other reasonably predicable natural conditions and is also supported by on-site back-up generators in the event of a power failure. All networking components and web and application servers are configured in a redundant configuration.

Informatica maintains a business continuity and disaster recovery program. Policies and procedures are in place to provide Cloud Services and Global Customer Support Services with minimal interruptions, including disaster recovery planning and testing capabilities, recovery site management and standard backup and recovery procedures. Informatica maintains geographically separate failover data centers for Cloud Services with a strict backup schedule for data at those facilities. Informatica's business continuity management system is aligned with ISO22301 and ISO31000 to prepare for, respond to, and recover from disruptive events.

Cyber Security

Informatica or an authorized third party performs periodic testing, including penetration testing, against Cloud Services available to the Internet. Informatica's security operations center, staffed by the office of Informatica's Chief Information Security Officer, is responsible for scanning and monitoring system activity and has pre-defined procedures for addressing or escalating vulnerabilities and events as needed. A security incident response team ("SIRT"), also staffed by the office of the Chief Information Security Officer, is responsible for investigating and responding to information-security related events escalated to their attention and determining if a Security Incident has taken place. Informatica Systems, including firewalls, routers, network switches and operating systems log information to enable the SIRT to detect, investigate, and resolve potential Security Incidents. Pre-defined procedures are also available to guide those efforts, including when to involve other internal groups in a response process and associated notification activities.

Insurance

Informatica maintains information security liability insurance or errors & omissions insurance covering liability for Security Incidents. Upon written request, Informatica will furnish to Customer a certificate of insurance evidencing required coverage and limits. In the event the policy is cancelled or modified before termination or expiration of the Agreement such that required coverage and limits are no longer met, Informatica will deliver notice of such cancellation or modification to Customer in accordance with Informatica's insurance policy provisions.

Transition of Services

Pursuant to mutually agreed upon license fees and hourly rates, Informatica shall reasonably cooperate to support an orderly transition of Maintained Customer Data to the services of another provider or to Customer's internal operations, which may include migrating Maintained Customer Data to Customer or its designee in a manner and format determined by Customer.

Disposition of Data

Informatica policy is to delete Maintained Customer Data within sixty (60) days of termination or expiration of Customer's subscription to the Cloud Service and to de-identify or delete Customer-specific Metadata within sixty (60) days of termination or expiration of Customer's subscription to the Cloud Service, solely except to the extent such Metadata are included in backup and disaster recovery logs the integrity of which requires that they remain unmodified. Informatica will promptly comply to the extent practicable with written requests to destroy Maintained Customer Data within shorter time periods than those indicated above and provide written certification of destruction of Maintained Customer Data upon Customer's written request.

Informatica policy is to delete Customer Data from Informatica Support Services systems upon termination of the Support Services investigation, including deletion of data from the secure FTP site, databases, hard drives, and virtual machines, and to delete the virtual meeting session.

Destruction of data as referenced herein includes, at minimum, secure erasure of media and secure disposal of records so that the information cannot be read or reconstructed.