Vendor Information Security Requirements (“Agreement”)

June 2023

Verint. Powering Actionable Intelligence. ®

Verint® is a global leader in Actionable Intelligence® solutions with a focus on customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in 180 countries—including over 80 percent of the Fortune 100—count on Verint solutions to make more informed, effective, and timely decisions.

Introduction

At Verint®, we recognize that the confidential information, intellectual property and all other information assets of Verint, Verint affiliates, Verint partners, and Verint customers and prospective customers (each a "**Verint Party**"), regardless of whether such information is in physical or electronic form (collectively, "**Information Assets**") are highly valuable assets and we are committed to protecting all Information Assets from unauthorized access or misuse. Therefore, as an integral part of the Third Party Code of Conduct, Verint has established the information security requirements set forth in this Agreement that must be adhered to by all Third Parties as a condition of any engagement with or for Verint (a "**Verint Engagement**"). By conducting business with Verint, each Third Party: **(i)** agrees that the requirements detailed in this Agreement are incorporated into each contract applicable to any Verint Engagement, and are binding on Third Party, and **(ii)** represents and warrants its continued compliance with this Agreement during any period of performance of any Verint Engagement. If you are entering into this Agreement on behalf of an organization, **(a)** all references to "Third Party" in this Agreement shall mean, and refer to, collectively you and your organization, and **(b)** you represent and warrant that you have full authority to bind that organization.

1. ACCESS TO INFORMATION ASSETS.

1.1 Permitted Access.

During any Verint Engagement, Verint Parties may provide Third Party with access to Information Assets. Third Party is only permitted to access Information Assets during the period of time Third Party is providing services to Verint Parties pursuant to the applicable Verint Engagement ("**Services**"). Third Party shall only authorize its employees and Verint approved subcontractors ("**Personnel**") to access Information Assets that have a need to know in order to perform Third Party's obligations applicable to the Verint Engagement. Third Party shall maintain a list of users that will use or have access to the Information Assets, including any changes to the list, and provide such list to Verint as requested from time to time. Third Party shall use its best efforts to prevent unauthorized access to Information Assets through the Third Party's systems. In no event shall Third Party place any equipment, devices or other physical attachments or any software or similar elements on the corporate computer network and/or other computing environments, computer systems and/or applications owned and/or licensed by a Verint Party for that Verint Party's business operations ("**Verint Network**") or a Verint Party's premises without the prior written consent of Verint. Third Party is prohibited from altering or modifying any aspect of Information Assets, unless Verint agrees in writing prior to such alteration or modification. For the avoidance of doubt, Information Assets include, without limitation, all Personal Data (defined in Section 1.5 below), all other Verint Party information and data of any form or type, Verint Network(s), and any hardware and/or software provided by a Verint Party.

1.2 Third Party's Systems.

Third Party must maintain a secure standard configuration on any machines accessing Information Assets. Such standard configuration shall meet Verint's current minimum requirements as updated and provided by Verint to Third Party from time to time, including, without limitation, VPN software and protocols, operating systems and versions, and the most current version and signature files of an industry best practice malware, anti-virus, anti-spyware and firewall products. Third Party will be responsible for procuring all systems required by Third Party to access and use Information Assets, including, without limitation, all hardware, software and third party services necessary for such access and/or required to satisfy Third Party's obligations in this Agreement and otherwise with respect to the applicable Verint Engagement. All systems used in providing any Services to Verint must be hardened to industry best practice.

1.3 SaaS Services.

In the event Third Party is using or providing any Verint Party with any ongoing cloud computing services, or other internet based services provided by Third Party as a part of a Verint Engagement ("**Cloud Services**"), in addition to all other obligations herein, Third Party will take all necessary steps to secure and prevent threats from impacting those Cloud Services, including, without limitation, the establishment of firewalls, intrusion detection and prevention, monitoring devices, backup and recovery practices, and other practices to prevent interruptions or degradation of the Cloud Services and protection of each applicable Information Assets. Third Party shall ensure the Cloud Services are available for the applicable Verint Party's intended use on a 24 x 7 basis, and that the minimum performance service levels are maintained. Third Party must continuously monitor its systems to ensure immediate detection and remediation of any incidents which may affect the Cloud Service.

1.4 Passwords; User IDs.

Third Party must comply with the password standards established by NIST 800-63 or equivalent, including, without limitation the use of "strong" passwords or multi factor authentication. Third Party's systems applicable to the Verint Engagement must be configured so **(i)** User IDs are disabled after five consecutive failed login

attempts, and **(ii)** User IDs that have been inactive for thirty (30) days must be disabled and User IDs that remain inactive for sixty (60) days must be deleted or blocked. Verint may, from time to time, issue User IDs and passwords to Third Party for accessing the Information Assets. For any passwords issued by Verint to Third Party, Third Party must immediately change that password upon initial logging into any Information Assets. All passwords and User IDs issued by Verint are deemed the confidential information of Verint. User IDs must not be disclosed to users not authorized to work on an applicable Verint Party's systems. User access must be secured if not in use by the authorized user. Third Party shall inform Verint immediately when any Personnel has left Third Party, is no longer performing on the Verint Engagement, or otherwise no longer requires access to the Information Assets.

1.5 Personal Data.

No Personal Data (defined below) of any Verint Party, its personnel or any third party is to be disclosed to any third parties, or transferred to another location (where the Verint Party has delivered Personal Data to Third Party), without the expressed written consent of Verint. Upon Verint's request, Third Party and any affiliate or subcontractor of Third Party shall enter into appropriate data transfer agreements with Verint as needed to satisfy cross-border transfer obligations relating to Personal Data (such as a data processing agreement, including, without limitation, the Standard Contractual Clauses) to allow Verint and its affiliates to transfer Personal Data to Third Party. Third Party shall encrypt, using industry standard encryption tools, all records and files containing Personal Data that Third Party: **(i)** transmits or sends wirelessly or across public networks, **(ii)** stores on storage media embedded in Third Party's systems, **(iii)** stores on laptops or other on portable devices, and/or **(iv)** stores on any device that is transported outside of the physical or logical controls of Third Party; provided, Third Party shall not store Personal Data on the device types specified in (iii) or (iv) without Verint's expressed written consent. Third Party shall safeguard the security and confidentiality of all encryption keys associated with encrypted Personal Data. If Third Party disposes of any Personal Data (regardless of form), Third Party shall do so by taking all reasonable steps to destroy that information by: **(a)** shredding; **(b)** permanently erasing and deleting; or **(c)** degaussing. "**Personal Data**" means and includes any account numbers (financial or otherwise), social security numbers, tax payer identification numbers, passport numbers, driver's license numbers and other government issued identification numbers, (ii) with respect to a payment card, the account holder's name, account number, service code, card validation code/value, PIN or PIN block, valid to and from dates and magnetic stripe data, information relating to a payment card transaction that is identifiable with a specific account, access codes to credit card and any other accounts, (iii) an individual's name or a unique identification number in combination with race, religion, ethnicity, medical or health information, background check information or sexual orientation, and any information resulting from a transaction with an individual or any service performed for an individual, and (iv) any other information concerning Verint employees, Verint vendor employees, and/or Verint customer employees and end customers. "**Standard Contractual Clauses**" means the contractual clauses approved by a Supervisory Authority pursuant to applicable privacy laws which provides for multi-jurisdictional transfer of Personal Data from one jurisdiction to another where such transfer would otherwise be a restricted transfer. "**Supervisory Authority**" means an independent public authority which is established in a jurisdiction under applicable privacy laws with competence in matters pertaining to data protection.

2. THIRD PARTY'S OBLIGATIONS.

2.1 Information Assets.

It is the policy of Verint that all information technology-based functions, facilities, and resources be designed, built, and operated in a manner that protects Information Assets. Third Party must take all actions necessary to ensure there are no intentional or accidental unauthorized use, access, disclosure, modification, damage, delay or removal of such Information Assets, and that any and all tangible and intangible rights, title and interest in and to intellectual property of a Verint Party and its licensors are protected. Verint's Information Security Management System is based on ISO 27001/27002, SSAE 18, and other recognized industry

standards in maintaining security and confidentiality of information, and obligates Third Party to maintain the equivalent standards with respect to Verint. In addition, the following are requirements with which Third Party is required to comply:

a. Third Party must maintain an information security policy that, at a minimum, includes **(i)** a definition of information security, its overall objectives and scope and the importance of security to Third Party, **(ii)** a statement of management intent, **(iii)** a framework for setting control objectives and controls, including the structure of risk assessment and risk management, **(iv)** a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization (including, without limitation, compliance with legislative, regulatory, and contractual requirements, security education, training, and awareness requirements, business continuity management and consequences of information security policy violations), **(v)** a definition of general and specific responsibilities for information security management, including, without limitation, reporting information security incidents, and **(vi)** references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules with which users must comply. Additionally, Third Party shall ensure that its information security policy covers all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones, and other devices and media that process or handle any Information Assets or that provide access to a Verint Network. Third Party's information security policy shall at a minimum provide the same levels of security and other requirements as specified by Verint from time to time, be consistent with all applicable Data Protection Requirements (defined below), satisfy the PCI Standards (to the extent applicable), and be consistent with prevailing industry practices. Additionally, Third Party must **(a)** implement appropriate controls to prevent unauthorized access of data, whether at rest or in transit, and **(b)** comply with its information security policy, and instructions or procedures, and Verint's instructions and procedures when directed, including Verint's policies and procedures communicated to Third Party from time to time. Further, Third Party shall **(x)** conduct its own internal audit no less than every twelve (12) months to verify and certify compliance, and **(y)** provide Verint with a copy of its information security policy and compliance certifications upon request, and **(z)** not modify its information security policy without the prior written consent of Verint. Any modifications to Third Party's information security policy must at a minimum provide the same level of protection previously provided. "**Data Protection Requirements**" as used in this Agreement means, collectively, all international, national, state and local laws or regulations relating to the protection of information that identifies or can be used to identify an individual, including, without limitation, as applicable with respect to Third Party's handling of Personal Data. "**PCI Standards**" as used in this Agreement, means the security standards for the protection of payment card data with which the payment card companies require merchants to comply, including, but not limited to, the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time.

b. Prior to the commencement date of any Verint Engagement, Third Party shall designate an individual as the primary security manager under this Agreement, and shall notify Verint on request of that individual's contact details. The security manager shall be responsible for managing and coordinating the performance of Third Party's obligations set forth in this Agreement. Additionally, Third Party shall maintain an incident response function with the capabilities to perform activities such as prevention, planning, detection, analysis, reporting, containment, investigation, eradication, recovery, and follow up of incidents such as root cause analysis and forensic research.

c. Third Party shall establish and maintain all standard application and system logs under its domain and further agrees that a copy of all logs shall be provided to Verint upon request. Third Party further agrees to permit Verint, upon reasonable request, to review and verify copies of relevant logs and data pertaining to any investigation performed by Verint regarding any incident for the purposes of protecting Information Assets.

2.2 Incidents.

If a disclosure, outbreak, violation or other breach of Third Party's obligations herein (an, "**Incident**") occurs, Third Party will promptly take all steps necessary to prevent any further damage to/exposure of any Information

Assets as well as any future Incidents, and will provide Verint with the relevant details of the steps taken to remediate against any further Incidents within one (1) business day of the Incident occurring. Further, and without prejudice to the foregoing, Third Party will take all actions necessary to immediately notify Verint via Verint's Privacy Portal (or other address or method as updated by Verint from time to time) of any Incident involving a breach of security that may have caused Information Assets to be disclosed to unauthorized third parties, and Third Party will use all best efforts to mitigate any costs, claims, damages and loss of Information Assets that may arise from the Incident. In the event such Incident concerns the disclosure of Personal Data, at the request of Verint, Third Party shall, or shall assist Verint's undertaking to issue notifications to any regulator with jurisdiction and to individuals impacted or potentially impacted by the Incident, and/or shall provide (or meet the cost of providing) any credit reporting service that Verint deems appropriate to provide to such individuals in order to mitigate the effect of the Incident on such individuals. Unless required by applicable law, Third Party shall not notify any individual or any third party other than law enforcement of any potential Incident involving Personal Data without first consulting with, and obtaining the permission of, Verint.

2.3 Use of Information Assets.

Verint grants to Third Party a non-exclusive, non-transferable right, revocable, limited right to access the Information Assets and use the information therein for the sole purpose of performing Services pursuant to the written contract applicable to the Verint Engagement, and Third Party acknowledges and agrees that: **(i)** Information Assets may only be used in connection with the provision of any Services as contemplated in this Agreement, and **(ii)** relevant governing or regulatory agencies, according to their respective charter and/or as required by law, and a Verint Party providing or making available Information Assets, may request an audit of Third Party's business practices when Personal Data or other customer information is accessed, held or protected by Third Party as though it were an extension of Verint, and Third Party agrees to consent to such request(s). Third Party shall at all times comply with and treat all Information Assets in accordance with the requirements of this Agreement and all Data Protection Requirements. Third Party will notify Verint in the event Third Party believes Verint's instructions concerning the Information Assets, or requirements of this Agreement, would cause Third Party or Verint to violate Data Protection Requirements. For the avoidance of doubt, Personal Data and information concerning Verint Networks are Verint confidential information.

2.4 Background Checks.

In addition to Verint's rights and Third Party's obligations elsewhere in this Agreement and/or in any other contract applicable to the Verint Engagement, in Verint's sole discretion, and where permitted by law, Verint may require Third Party's Personnel undergo Tests (defined below) by a third party agency selected by Verint which may also include investigation of Third Party's Personnel's employment history, educational background, and department of motor vehicle records. In the event that the results of any Test is not satisfactory to Verint, Third Party hereby agrees that Verint shall have the right, in its sole discretion, to request immediate removal of such Personnel and Third Party shall promptly comply. In addition to (and without limiting) the foregoing, prior to assigning any of its Personnel to positions in which they will, or may reasonably be expected to, have access to Information Assets, or physical access to Verint facilities, Third Party shall conduct a Background Check on such Personnel. Upon request by Verint, Third Party shall provide to Verint the results of Test(s) performed by Third Party (which Verint may disclose as required by a relevant governing or regulatory agency, or Verint customer), and shall re-perform such Test(s) as reasonably requested by Verint. Third Party shall not permit any person who has failed a Drug Test or Background Check to perform on a Verint Engagement. If Third Party's Personnel fail a Drug Test or Background Check subsequent to the date they first perform on a Verint Engagement, or Third Party learns of a prior conviction during the period of performance of any Verint Engagement, Third Party will inform Verint of the specifics of such change and remove such person from performing any services for Verint, unless otherwise requested by Verint in writing. **"Tests"** means collectively, Background Checks and Drug Tests, with each individually being referred to as a "**Test**". "**Background Check**" means a check to determine whether a person has been convicted of, or entered into a pre-trial diversion program arising from prosecution with respect to: **(a)** any felony; or **(b)** any misdemeanor or other

crime involving dishonesty, breach of trust, money laundering, or moral turpitude (including without limitation embezzlement, fraud, securities or financial related crime, perjury, money laundering, larceny, or illegal manufacture, sale, distribution, or trafficking in controlled substances), but may also include other checks. "**Drug Test**" means a ten (10) panel drug testing screen (or as otherwise specified by Verint).

2.5 Third Party's Personnel.

Third Party certifies that its Personnel have been and shall continue to be provided with a clear understanding of the necessary procedures and controls to comply with the terms of this Agreement and the security requirements set forth herein. Third Party shall: **(a)** maintain appropriate access controls, including, but not limited to, limiting access to Information Assets to the minimum number of Personnel who require such access in order to provide the Services, **(b)** require its Personnel who will be provided access to, or otherwise come into contact with, Information Assets to protect such Information Assets in accordance with the requirements of this Agreement, **(c)** provide such Personnel with appropriate training regarding information security and the protection of personal information, and **(d)** require its Personnel to attend training required by Verint.

2.6 Subcontractors.

Unless Verint provides its expressed written consent with respect to specific individuals from Third Party's subcontractors, Third Party may not use any individuals other than Third Party's own employees to access and/or use Information Assets. In the event Verint provides such expressed written consent, Third Party agrees **(i)** to maintain a vendor security process to ensure that appropriate due diligence is conducted prior to utilizing such subcontractors to provide any services hereunder, including compliance with all obligations hereunder, **(ii)** to monitor on an ongoing basis the security capabilities and compliance of any such subcontractors with the terms and conditions of this Agreement, and **(iii)** Third Party is jointly and severely liable for the acts and/or omissions of that subcontractor.

2.7 Use of Systems.

Third Party agrees to not, and shall ensure its Personnel do not **(i)** store or communicate unlawful, abusive, defamatory, obscene, pornographic, profane, indecent information of any kind on or through a Verint Network, **(ii)** scan network or systems, monitor network traffic, **(iii)** use pirated software or software that does not have a license, or infringe on any copyrights, trademarks, or any other proprietary rights, **(iv)** alter, damage, copy or delete any Information Assets, **(v)** interfere with the ability of the Verint Network to function normally, and **(vi)** unless expressly authorized by a relevant Verint Party, access any Verint Party systems or networks to which Verint connects.

2.8 Indemnity.

Third Party shall indemnify and hold harmless each Verint Party, and its affiliates, and its and their officers, directors, employees, agents, successors, assigns, and subcontractors from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including attorneys' fees and court costs) arising from or in connection with Third Party's breach of its obligation in this Agreement.

2.9 Monitoring.

Third Party acknowledges and agrees that a Verint Party may monitor any and all activity performed by Third Party and its Personnel while on the Verint Network, and may audit Third Party's systems to verify compliance with this Agreement. In the event Verint determines or has reasonable suspicions of a violation of this Agreement, Verint may, without notice, block or remove Third Party access.