

## VENDOR INFORMATION SECURITY REQUIREMENTS

### 1. ACCESS TO INFORMATION ASSETS.

#### 1.1 Permitted Access.

During the term of the Agreement, Verint Parties may provide Contractor and its Personnel with access to the Information Assets. Contractor is only permitted access to Information Assets during the period of time Contractor is providing Services to Verint Parties hereunder. Contractor shall only authorize its Personnel to access Information Assets that have a need to know in order to perform Contractor's obligations under the Agreement. Contractor shall maintain a list of users that will use the Information Assets, including any changes to the list, and provide such list to Verint as requested from time to time. Contractor shall use its best efforts to prevent unauthorized access to Information Assets through the Contractor's systems. In no event shall Contractor place any equipment, devices or other physical attachments or any software or similar elements on the Verint Network or premises without the prior written consent of Verint. Contractor is prohibited from altering or modifying any aspect of Information Assets, unless Verint agrees in writing prior to such alteration or modification.

#### 1.2 Contractor Systems.

Contractor must maintain a secure standard configuration on any machines accessing Information Assets. Such standard configuration shall align to industry best practice frameworks including but not limited to NIST CsF, ISO 27001, and other standards. Contractor will be responsible for procuring all systems required by Contractor 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 Contractor's obligations in the Agreement. All systems used in providing any Services to Verint must be hardened to industry best practice.

#### 1.3 SaaS Services.

In the event Contractor is using or providing any Verint Party with Cloud Services as a part of its performance hereunder, in addition to all other obligations herein, Contractor 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 Service and protection of each applicable Verint Party's Information Assets. Contractor 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 services levels are maintained. Contractor must continuously monitor its systems to ensure immediate detection and remediation of any incidents which may affect the Cloud Service. Contractor will provide non-qualified SSAE 18 SOC 2 or SOC 3 report covering the Trust Services Principles (TSP) of security, availability, processing integrity, and confidentiality. If Contractor is processing Personal Data, Contractor will include the privacy TSP. Contractor will provide a Type I report within six (6) months of executing this agreement. Contractor will provide a Type II report within 18 months of executing this agreement. Contractor will make available the audit reports no more than once per year upon request. Failure to provide a non-qualified audit report will be considered a breach of this agreement.

#### 1.4 Passwords; User IDs.

Contractor must comply NIST 800-63B. Contractor's systems applicable to the Agreement 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 Contractor for accessing the Information Assets. For any passwords issued by Verint to Contractor, Contractor 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 authorized user. Contractor shall inform Verint immediately when any Personnel has left Contractor, is no longer performing under the Agreement, or otherwise no longer requires access to the Information Assets.

#### 1.5 Personal Data.

No Personal Data 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 Contractor), without the expressed written consent of Verint. Upon Verint's request, Contractor and any affiliate or subcontractor of Contractor 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, or other similar agreements relating to other countries) to allow Verint and its affiliates to transfer Personal Data to Contractor. Contractor shall encrypt, using industry standard encryption tools, all records and files containing Personal Data that Contractor: (i) transmits or sends wirelessly or across public networks, (ii) stores on storage media embedded in Contractor's systems, (iii) stores on laptops or other on portable devices,

and (iv) stores on any device that is transported outside of the physical or logical controls of Contractor; provided, Contractor shall not store Personal Data on the device types specified in (iii) or (iv) without Verint's expressed written consent. Contractor shall safeguard the security and confidentiality of all encryption keys associated with encrypted Personal Data. If Contractor disposes of any Personal Data (regardless of form), Contractor shall do so by taking all reasonable steps to destroy that information by using methods described in NIST 800-88 or equivalent standards.

### 2. CONTRACTOR 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. Contractor 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 the Intellectual Property Rights of a Verint Party and its licensors are protected. Verint Information Security Management System is based on ISO 27001 Standards in maintaining security and confidentiality of information, and obligates Contractor to maintain the equivalent standards with respect to Verint. Contractor will provide its security certifications and external audit reports upon request but no more than once per year. In addition, the following are requirements with which Contractor is required to comply:

a. Contractor must maintain an Information Security Policy. Contractor 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 a Verint Party's Information Assets or that provide access to a Verint Network. Additionally, Contractor must implement appropriate controls to prevent unauthorized access of data, whether at rest or in transit. Contractor's Information Security Policy shall at a minimum align to best practice frameworks in 1.2, be consistent with all applicable Data Protection Requirements, satisfy the PCI Standards (to the extent applicable), and be consistent with prevailing industry practices. Contractor must comply with its Information Security Policy, and instructions or procedures. Contractor shall conduct its own internal audit no less than every twelve (12) months to verify and certify compliance. Contractor shall provide Verint with a copy of its Information Security Policy and compliance certifications upon request. Any modifications to Contractor's Information Security Policy must at a minimum provide the same level of protection previously provided.

b. On the effective date of the Agreement, Contractor shall designate an individual as the primary security manager under the 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 Contractor's obligations set forth in this Schedule. Contractor 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. Contractor 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. Contractor 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 an Incident occurs, Contractor 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, Contractor will take all actions necessary to immediately notify Verint via Verint's [Privacy Portal](#) of any Incident involving a breach of security that may have caused Information Assets to be disclosed to unauthorized third parties, and 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, Contractor 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 law, Contractor 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 Contractor a non-exclusive, non-transferable right, revocable, limited right to access the Information Assets and use the information therein for the sole purposes of performing Services under the Agreement, and Contractor acknowledges and agrees that: (i) Information Assets may only be used in connection with the provision of any Services as contemplated in the 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 Contractor's business practices when Personal Data or other customer information is accessed, held or protected by Contractor as though it were an extension of Verint, and Contractor agrees to consent to such requests. Contractor shall at all times comply with and treat all Information Assets in accordance with the requirements of this Schedule and all Data Protection Requirements. Contractor will notify Verint in the event Contractor believes Verint's instructions concerning the Information Assets, or requirements of this Schedule, would cause Contractor or Verint to violate Data Protection Requirements.

#### **2.4 Background Checks.**

In addition to any of Verint's rights and Contractor's obligations elsewhere in the Agreement, 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, Contractor shall conduct a Drug Test and Background Check and allow Verint to conduct a Background Check on such Personnel. Contractor shall not permit any person to perform under the Agreement who has failed a Test. If Contractor's Personnel fail a Test subsequent to the date they first perform under the Agreement, or Contractor learns of a prior conviction during the term of the Agreement, Contractor 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. Upon request by Verint, Contractor shall provide to Verint the results of Tests (which Verint may disclose as required by a relevant governing or regulatory agency, or Verint customer), and shall re-perform such Tests as reasonably requested by Verint.

#### **2.5 Contractor Personnel.**

Contractor 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 the Agreement and the security requirements set forth herein. Contractor 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 the Agreement and the security requirements set forth herein, (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 Contractor's subcontractors, Contractor may not use any individuals other than Contractor's own employees to access and/or use Information Assets. In the event Verint provides such expressed written consent, Contractor 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 the Agreement, including but not limited to the requirements set forth herein, and (iii) Contractor is jointly and severally liable for the acts and/or omissions of that subcontractor.

#### **2.7 Use of Systems.**

Contractor 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.**

Contractor 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 Contractor's breach of its obligation in this Schedule.

#### **2.9 Monitoring.**

Contractor acknowledges and agrees that a Verint Party may monitor any and all activity performed by Contractor and its Personnel while on the Verint Network, and may audit Contractor's systems to verify compliance with this Schedule. In the event Verint

determines or has reasonable suspicions of a violation of this Schedule, Verint may, without notice, block or remove Contractor access.

#### **2.10 Business Continuity**

Contractor will maintain a business continuity and disaster recovery plan that aligns with ISO 22301, NIST 800-34, and other best practice frameworks. Contractor will provide a high level summary of its plans upon request but no more than once per year.

### **3. DEFINITIONS.**

#### **3.1 Cloud Services.**

Any ongoing cloud computing Services, or other internet-based Services provided by Contractor as a part of their performance.

#### **3.2 Confidential Information.**

Any non-public information, technical data, or know-how, including, without limitation, that which relates to a disclosing party's: (i) research, product plans, products, pricing, services, customers, personnel, markets, software, software code, software documentation, developments, inventions, lists, trade secrets, data compilations, processes, designs, drawings, engineering, hardware configuration information, marketing or finances, which is designated in writing to be confidential or proprietary at the time of disclosure, or regardless of form or designation is otherwise expressed to be confidential or proprietary information hereunder or is information the receiving party should reasonably understand to be confidential or proprietary, because of its very nature, (ii) Personal Data, (iii) information concerning Verint Networks, and (iv) the terms and conditions of this Schedule. Notwithstanding the foregoing, Confidential Information does not include information, technical data or know-how that, without restriction on disclosure, is: (a) in the public domain or becomes available to the public and not as a result of the act or omission of the receiving party; (b) rightfully obtained by the receiving party from a third party; (c) lawfully in the possession of the receiving party at the time of disclosure; or (d) approved for release by written authorization of the disclosing party.

#### **3.3 Data Protection Requirements.**

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 Contractor's handling of Personal Data.

#### **3.4 Incident.**

A disclosure, outbreak, violation, or other breach of Contractor's obligations herein.

#### **3.5 Information Assets.**

All Intellectual Property and Confidential Information of any Verint Party, regardless whether in physical or electronic form, and including, without limitation, all Personal Data 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.

#### **3.6 Information Security Policy.**

An information security policy that outlines a definition of information security, its overall objectives and scope and the importance of security to Contractor; a statement of management intent; a framework for setting control objectives and controls, including the structure of risk assessment and risk management; 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); a definition of general and specific responsibilities for information security management, including, without limitation, reporting information security incidents; 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.

#### **3.7 Intellectual Property.**

Includes: (i) works of authorship, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademarks and trade names, (iii) Confidential Information, trade secrets and know-how, (iv) patents, designs, algorithms and other industrial property, (v) all other intellectual and industrial property rights whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force.

#### **3.8 Intellectual Property Rights.**

Any and all tangible and intangible rights, title and interest in and to Intellectual Property.

**3.9 Personal Data.**

(i) All 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 Parties employees, Verint Parties vendor employees, and/or Verint Parties customer employees and end customers.

**3.10 Personnel.**

Each of Contractor's employees, Verint approved subcontractors and other individuals and entities performing hereunder for Contractor.

**3.11 Services.**

All agreed-upon services provided by Contractor to a Verint Party.

**3.12 Standard Contractual Clauses.**

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.

**3.13 Supervisory Authority.**

An independent public authority which is established in a jurisdiction under applicable privacy laws with competence in matters pertaining to data protection.

**3.14 Test.**

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).

**3.15 Verint Network.**

The corporate computer network and other computing environments, computer systems and/or applications owned and/or licensed by a Verint Party for that Verint Party's business operations.

**3.16 Verint Parties.**

Any one or more of the following entities (as applicable): Verint, Verint affiliates, Verint partners, and Verint customers and prospective customers.