INFORMATION SECURITY SCHEDULE

1 DEFINITIONS.

1.1 Customer Data. All data provided by Customer to Verint where such data contains Personal Data, or with respect to Hosted Services, data collected or generated by Hosted Services on Customer's behalf, and remains in Verint's possession and control for further Processing.

1.2 Encryption Standards. Encryption algorithms that are publicly or commercially available, with key lengths sufficient to prevent commercially reasonable attempts to decrypt through brute force the encrypted information.

1.3 Hosted Services. Any SaaS services and other Verint provided hosted services subscribed to by Customer.

1.4 Industry Standards. Generally accepted standards applicable to the performance obligations of a party with respect to a product or service. Industry Standards can include in part or in whole frameworks published by the National Institutes for Standards and Technology (NIST), International Organization for Standardization, ISACA, Payment Card Industry Security Standards Council and other internationally recognized standards organizations.

1.5 Personal Data. Any information relating to an identified or identifiable natural person; 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.

1.6 Privacy Laws. Laws, as applicable, concerning the regulation of personal information about individuals sufficient to identify such individuals.

1.7 Process(ing)(ed). Any operation or set of operations that is performed on Personal Data, including, without limitation, collection, recording, retention, alteration, use, disclosure, access, transfer or destruction.

1.8 Verint Personnel. Each Verint employee or subcontractor under obligations of confidentiality and nondisclosure which performs on behalf of Verint hereunder.

2 GENERAL SECURITY TERMS. Verint is committed to helping protect the security of Customer Data, and has implemented, and will maintain and follow appropriate technical and organizational measures that conform to Industry Standards intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. Verint may modify any of its policies, process or procedures at any time and without obligation to notify or update this Schedule, provided such modifications provide substantially similar or greater protections than those provided for herein. Except as otherwise specified in the Agreement or in Section 3 this Schedule, the following terms and conditions in this Section 2 apply to all performance obligations under the Agreement.

2.1 Access Controls. Verint implements Industry Standard access control methodologies, which rely on policy, process, and logical controls to help prevent unauthorized access to systems and data under Verint's control. These access controls include no less than the following:

- Verint uses the "Principle of Least Privilege" model for restricting access to systems and data, and regularly reviews access rights granted to Verint Personnel.
- Verint Personnel each have a unique user ID and personal secret password for accessing internal networks, equipment and data. Verint shall maintain policies concerning the maintenance of password secrecy. Verint Personnel access rights must be suspended within twenty-four (24) hours of employment termination, and modified within forty-eight (48) hours when Verint Personnel roles and/or responsibilities are changed.
- Verint maintains a password policy which, at a minimum, complies with the following standards: **(i)** passwords must not employ any structure or characteristic that results in a password that is predictable or easily guessed; **(ii)** passwords must include at least three (3) of the following character sets, in accordance with password policy settings: **(a)** an English uppercase character (A – Z); **(b)** an English lowercase character (a – z); **(c)** a westernized Arabic numeral; and **(d)** a non-alphanumeric special character from the following character set: !, $, #, %; **(iii)** passwords must be changed at least every one hundred and eighty (180) days; and **(iv)** account lockout must occur after a maximum of five (5) failed password entry attempts. Re-enabling of locked accounts must require extended time based delay, or interaction with a security administrator or help desk function. All password changes must be accomplished through secure procedures.
- Multi-factor authentication processes must be utilized for any access to systems containing Customer Data. All passwords must be stored and transmitted using Encryption Standards.
- User sessions must expire and require the re-entry of a password if idle by more than **(i)** twenty (20) minutes for administrator consoles, and (ii) sixty (60) minutes for all other systems and session types.
- For any facilities hosting Customer Data, such facilities shall have implemented electronic access controls to enter such facilities, and further access controls for entering specific areas where such Customer Data is physically resident. Verint shall maintain processes to validate the identity of individuals prior to issuing identification and access badges, and shall maintain processes for issuing visitor badges, logging such issuance, and escort requirements for such visitors. Such logs shall be maintained by Verint for no less than six (6) months from issuance.

2.2 Data Controls. In its performance obligations, Verint does not require access to Customer systems or data, and Customer shall take commercially reasonable efforts to prevent Verint from accessing Customer systems and data. Where Customer provides Customer Data to Verint for professional services or support purposes, Customer shall take commercially reasonable efforts to redact or remove Personal Data prior to providing that Customer Data to Verint. Where possible, such services shall be delivered via screen share or telephone with no data transferred to Verint. If it is necessary to transfer Customer Data to Verint, the following shall apply:

- Customer shall only use Verint approved communication channels for providing Customer Data to Verint. With respect to the storage of such Customer Data by Verint and any further transmission of that Customer Data by Verint, Verint shall ensure such Customer Data is protected using Encryption Standards.
- In the event Verint makes backups of such Customer Data, all backups of Customer Data shall be encrypted on backup media using Encryption Standards.
- Customer Data may only be stored on portable media, including laptops, DVD, CD, magnetic tape media, removable hard drives, USB drives or similar portable storage, if Encryption Standards are used on that portable media.

2.3 Operational Controls. Verint shall maintain operational controls sufficient to enable Verint's satisfaction of its performance obligations in this Section 2, including, without limitation, the following:

- Maintain a dedicated information security function to design, maintain and operate security in line with Industry Standards. This function shall focus on system integrity, risk acceptance, risk analysis and assessment, risk evaluation, and risk management.
- Maintain a written information security policy that is approved by the Verint management team and published and communicated to all Verint Personnel and relevant third parties.
- Provide security awareness training at least annually to its employees, and maintain records of training attendance for no less than one (1) year.
- Conduct vulnerability assessments and/or penetration tests of networks, systems, applications and databases where Customer Data is located at rest, in transit and in use. Verint shall triage identified vulnerabilities and remediate or mitigate vulnerabilities in accordance with Industry Standards.
- Maintain appropriate authentication system(s) to authenticate and restrict access to Verint systems and networks to valid users.

- Install and maintain antivirus software on all servers and computing devices involved with Processing activities, and use other malware detection techniques where reasonably required. Such antivirus software shall be updated on a daily basis, or as otherwise provided by the antivirus software manufacturer.
- Maintain physical security measures with respect to Verint facilities to help prevent and detect physical compromise, including, without limitation, use of identification badges, smart card or other electronic or physical identity verification systems, alarms on external doors, and CCTV on all entrances / exits to such facilities. Verint shall periodically review access records and CCTV video to ensure access controls are being enforced effectively, with any discrepancies or unauthorized access investigated immediately.
- With respect to Verint internal networks, ensure perimeter networks are physically or logically separated from internal networks containing Customer Data, establish and configure firewalls in accordance with Industry Standards, use network intrusion detection systems as a part of network security, and restrict and control remote network access.
- Complete diligent review of any Verint subcontractors that will have access to Customer Data, and require such subcontractors contractually commit to substantially similar terms and conditions as those specified in this Schedule, or terms and conditions that Verint reasonably determines as providing substantially similar protection. With respect to any performance subcontracted by Verint, Verint remains responsible for its subcontractors' compliance with Verint's performance obligations in the Agreement.

2.4 Availability Controls. Verint will maintain contingency planning policies and procedures defining roles and responsibilities on proper handling of contingency events. This shall include a business continuity and disaster recovery plan intended to facilitate the restoration of critical operations and processes which would allow for Verint's continued performance of its obligations hereunder. Such plan shall be periodically reviewed, updated and tested by Verint.

2.5 Application Controls. Verint shall implement and conform its software development practices to applicable Industry Standards relative to the functionality to be performed by the specific Verint product offering. Verint shall maintain software development practices which satisfy the following:

- Use commercially reasonable measures to detect product vulnerabilities prior to release. These measures may include manual test scripts, test automation, dynamic code analysis, static code analysis, penetration testing, or other measures chosen by Verint. Verint shall update procedures and processes from time to time to improve detection of vulnerabilities within its products.
- Verint's developers shall not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any systems or network.
- Verint's developers shall receive regular training on coding and design with respect to application security.

3 SAAS AND HOSTING SECURITY TERMS. In addition to the terms and conditions in Section 2, the following terms and conditions shall apply to Verint's performance obligations with respect to any Hosted Services procured by Customer under the Agreement. To the extent of any conflict between the terms and conditions in this Section 3 and in Section 2, the terms and conditions in this Section 3 shall control solely with respect to Hosted Services.

3.1 Access Controls. Customer shall have access to Customer Data maintained within their applicable production instance. Customer shall be responsible for maintaining user access and security controls for users accessing the Hosted Services. Verint shall be responsible for restricting all other access to Customer Data residing within the production instance. For the avoidance of doubt, Verint has no obligation to verify that any user using Customer's account and password has Customer's authorization. Verint shall provide access on a need to know basis and shall review access rights of Verint Personnel at least annually. Verint's access controls shall include no less than the following:

- Verint shall enforce complex passwords using built in system settings of at least 8 characters. Verint shall require password changes at least every ninety (90) days. Verint administrators shall use multi-factor authentication for access to the production environment(s).
- Access to Verint's production environment(s) is controlled at four distinct hierarchical levels: the hosting partner level, the SaaS operations team level, the Verint network security level, and the application level. Access control is required for each of these levels to provide the optimal level of security for the solution.
- Any Customer Data accessed by authorized Verint Personnel, is subject to the aforementioned access controls and is encrypted at rest and in transit.
- A Verint hosting partner's role is to design, deploy, secure, make available, and support the infrastructure upon which Hosted Services operate. For the avoidance of doubt, "hosting partner" shall mean the Sub-processors providing Hosted Services infrastructure specified in an Order or the Data Processing Instructions. The hosting partners have primary control over the infrastructure upon which Hosted Services operate but such control does not extend to access to Customer Data or Verint solutions processing Customer Data. The hosting partner provides Verint's operations teams with the initial credentials required to access the infrastructure and associated support portals to enable Verint to operate and manage the Hosted Services.

3.2 Data Controls. In its performance obligations with respect to Hosted Services, Verint does require access to Customer Data, and the following additional terms and conditions shall apply:

- Verint's security procedures shall require that any Customer Data stored by Verint only be stored using secure data encryption algorithms and key strengths of 128-bit symmetric and 1024-bit asymmetric or greater. Verint shall monitor Industry Standards and implement an action plan if key lengths in use can be compromised through commercially reasonable means.
- Verint will maintain a key management process that includes appropriate controls to limit access to private keys and a key revocation process. Private keys, and passwords shall not be stored on the same media as the data they protect.
- Verint will prohibit Verint Personnel from the download, extraction, storage or transmission of Customer Data through personally owned computers, laptops, tablet computers, cell phones, or similar personal electronic devices except where enrolled in Verint's Mobile Device Management (MDM), Information Rights Management (IRM), or other security programs. If personal computers or mobile devices are used to perform any part of the Hosted Services, Verint will encrypt all Customer Data on such mobile devices.
- Verint agrees that any and all Verint initiated electronic transmission or exchange of Customer Data stored as part of the Hosted Services shall be protected by a secure and encrypted means (e.g. HTTPS, PGP, S/MIME, SSH, SMTP encryption using TLS on gateway while sending emails).
- Customer Data stored as a part of the Hosted Services shall reside only on Verint production systems housed in Verint hosting partner data centers, unless noted in an Order or statement of work or required with respect to professional service engagements or performance of support services. Any storage of Customer Data on Verint premises is temporary and is used strictly for support and services engagements. Once Customer Data on Verint premise has served its purpose, it shall be promptly destroyed in accordance with Verint's confidential data destruction procedures.

3.3 Operational Controls. In its performance of Hosted Services, Verint shall maintain operational controls sufficient to enable Verint's satisfaction of its performance obligations in this Section 3, including, without limitation, the following:

- Verint will utilize up-to-date and comprehensive virus and malware protection capabilities, and commercially reasonable practices, including detection, scanning and removal of known viruses, worms and other malware on the Verint's hosting systems. These virus protection capabilities will be in force on all computers and/or devices utilized in connection with the technology services, as well as on all data files or other transfers that have access or are connected to Verint's hosting system.
- If a virus, worm or other malware causes a loss of operational efficiency or loss of data, Verint will mitigate losses and restore data from the last virus free backup to the extent practicable.

- Verint shall obligate its hosting partners to provide a multiple layered security approach. This shall include perimeter firewalls, DMZ, one or more internal network segments, and network intrusion detection monitors for attempted intrusion to the production environment. Network vulnerability scans shall be conducted regularly and issues addressed according to Industry Standard change control processes.
- Verint shall mitigate security vulnerabilities through the use of perimeter and host countermeasures such as intrusion prevention, web application firewall, IP address shunning, and other measures designed to prevent successful exploitation of vulnerabilities.
- Verint and its hosting partners shall proactively address security risks by applying released security patches, including, as example, Windows security patching and updates to patch known vulnerabilities in an applicable operating system. Patches shall be deployed to production via Verint's change management process. Verint shall test all patches in its test environment prior to release to production. If a patch degrades or disables the production environment, Verint shall continue to mitigate vulnerabilities until a patch is provided by the software or operating system manufacturer that does not degrade or disable production. Such mitigation efforts may include intrusion prevention, web application firewall, and other measures chosen by Verint to reduce likelihood or prevent successful access to Customer Data by an unauthorized party.
- Each month, Verint and its hosting partners shall schedule maintenance windows to perform data center, system, and application maintenance activities. Verint shall notify Customer in advance of any scheduled maintenance activity that is expected to disrupt the Hosted Services functionality.
- Verint shall retain security logs for a minimum of thirty (30) days online and ninety (90) days archived. Verint may retain logs for a longer period at its sole discretion.

3.4 **Availability Controls.** With respect to Hosted Services:

- Verint shall maintain business continuity and disaster recovery plans specific to its Hosted Services, and shall include data center failover configurations.
- Verint shall maintain a backup of all Customer Data that Verint is required to retain as a part of the Hosted Services. In the event the Customer Data becomes corrupt, Verint shall use commercially reasonable efforts to remediate and recover such corrupt data.

3.5 **Audit.** Except as otherwise required under local laws or regulations applicable to the Hosted Services, the following terms and conditions shall apply. With respect to Verint operations applicable to Hosted Services, Verint conducts internal and external 3rd party audits on a regularly scheduled basis. Verint shall correct any material deficiencies noted in an audit report within a commercially reasonable timeframe and shall request auditor to provide an updated report reflecting successful corrective actions. Customer may request executive summaries of these audit reports no more than annually. Verint reserves the right to redact Confidential Information from the reports prior to sharing.

4 **ATTESTATIONS OF COMPLIANCE.** Upon Customer's reasonable request, **(i)** Verint shall provide an attestation of compliance to the terms in this Schedule, and/or **(ii)** Verint shall provide its Industry Standard security assessment questionnaire responses applicable to the services provided to Customer. Requests shall be made in writing through the Account Executive assigned to Customer unless otherwise specified by Verint.