INFORMATION SECURITY SCHEDULE

1 DEFINITIONS.

1.1 Back Office Systems. Verint's internal technical environment, IT systems and networks used to implement and manage the Hosted Environment or that are used to access Customer Data.

1.2 Customer.

The organization named as customer in the agreement to which this Information Security Schedule forms a part.

1.3 Customer Data. All content and data, including but not limited to Personal Data, either provided by Customer or entered on its behalf, in either case, through use of the SaaS Services, or collected or generated by the SaaS Services on behalf of Customer, and which remains in Verint's possession and control for further Processing.

1.4 Data Processing Instructions.

The data processing instructions set out at set out at https://www.verint.com/wp-content/uploads/Verint-Data-Processing-Instructions.pdf.

1.5 Encryption Controls. Encryption algorithms that are publicly or commercially available with sufficient key lengths in accordance with Industry Standards to prevent commercially reasonable attempts to decrypt through brute force the encrypted information.

1.6 Hosted Environment. Verint or its third party's technical environment required to operate and provide access to the relevant SaaS Services.

1.7 Industry Standards. Generally accepted industry security standards applicable to the performance obligations regarding Processing of Customer Data. 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.

1.8 Personal Data. Any information relating to an identified or identifiable natural person ("Data Subject"); 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.

1.9 Personnel. With respect to Customer, (i) each of Customer's and/or Customer's Affiliate's employees and independent contractor (in each case, not a competitor of Verint) under obligations (a) of confidentiality and nondisclosure, and (b) to protect Verint Intellectual Property, and (ii) any other individuals with access to components of the SaaS Service designated for external use, which Customer authorizes to use the SaaS Services purchased; with respect to Verint, each Verint employee or subcontractor under obligations of confidentiality and nondisclosure which performs on behalf of Verint hereunder. For the avoidance of doubt, each party shall be responsible for its Personnel's compliance with this Agreement.

1.10 Privacy Laws. National, federal, union, state and other laws, as applicable, to the Processing of Personal Data.

1.11 Process(ing)(ed). Any operation or set of operations that is performed upon Personal Data in connection with the SaaS Services, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction as described in this Agreement and the Data Processing Instructions.

1.12 SaaS Services. The online services offered by Verint as more fully described in the Verint documentation as subscribed to under the Agreement and each relevant order.

1.13 Verint. The Verint entity named in the agreement to which this Information Security Schedule forms a part.

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 when Processing. Verint may modify any of its policies, process or procedures at any time provided that such modifications provide greater or substantially similar protections than those provided for in this Schedule.

3 BACK OFFICE SYSTEMS SECURITY AND BUSINESS CONTINUITY.

3.1 Access Controls. Verint implements Industry Standard access control methodologies in respect of Back Office Systems, which rely on policy, process, and logical controls to prevent unauthorized access. These access controls include no less than the following:

- Multi-factor authentication processes must be utilized for any access to Back Office Systems. All passwords must be stored and transmitted using Encryption Controls.
- Verint uses the "Principle of Least Privilege" model for restricting access Back Office Systems and regularly reviews access rights granted to Verint Personnel.
- Verint Personnel each have a unique user ID and personal secret password for accessing Back Office Systems which are subject to 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 conforms to ISO27001 and NIST 800-63B or equivalent Industry Standards.
- User sessions must expire and require the re-entry of a password if left in an idle state.

3.2 Data Controls. Where Customer provides Customer Data to Verint for Professional Services 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 secure screen share controlled by Customer with no Customer 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 Controls.
- In the event Verint makes backups of such Customer Data, all backups of Customer Data shall be encrypted using Encryption Controls.

3.3 Operational Controls. Verint shall maintain operational controls to further protect Back Office Systems 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.
- 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 all Back Office Systems involved with Processing activities.

- Maintain physical security measures with respect to Verint managed 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.
- 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 Back Office Systems, 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.

3.4 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 which are dependent on Back Office Systems. Such plan shall be periodically reviewed, updated and tested by Verint.

3.5 Application Controls. Verint shall implement and conform its software development and implementation practices to applicable Industry Standards relative to the functionality to be performed by the specific Verint product offering comprised in the SaaS Services 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.

4 HOSTED ENVIRONMENT SECURITY AND BUSINESS CONTINUITY. Verint implements Industry Standard access control methodologies in respect of the Hosted Environment which rely on policy, process, and logical controls to prevent unauthorized access. These access controls include no less than the following.

4.1 Access Controls. Customer shall have access to Customer Data maintained within their applicable Hosted Environment. Customer shall be responsible for maintaining user access and security controls for users accessing the SaaS Services. Verint shall be responsible for controlling and restricting all other access to Customer Data residing within the applicable Hosted Environment. For the avoidance of doubt, Verint has no obligation to verify that any Customer Personnel using Customer's account and password has Customer's authorization. Verint shall provide access to the Hosted Environment in order to comply with its performance obligations under the Agreement and maintain access controls which shall include no less than the following:

- Verint shall enforce complex passwords using built in system settings of at least 12 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).
- Verint uses the "Principle of Least Privilege" model for restricting access the Hosted Environment and regularly reviews access rights granted to Verint Personnel.
- Customer Data stored in the Hosted Environment is subject to Encryption Controls at rest and in transit within the Hosted Environment.
- Verint's cloud services vendors provide the infrastructure upon which the Hosted Environment operates. Such vendors have primary control over the infrastructure upon which the Hosted Environment operates but such control does not extend to permit access to Customer Data or Processing Customer Data.

4.2 Data Controls. In its performance obligations with respect to the Hosted Environment, the following additional terms 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 256-bit symmetric and 2048-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.
- Verint agrees that any and all Verint initiated electronic transmission or exchange of Customer Data stored within Hosted Environment 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).

4.3 Operational Controls. Verint shall maintain operational controls sufficient to enable Verint's satisfaction of its performance obligations in this Section 4, 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 Hosted Environment
- 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 ensure that its cloud services vendors 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. 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 cloud service vendor 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.

- 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.

4.4 **Availability Controls.** With respect to the Hosted Environment:

- Verint shall maintain business continuity and disaster recovery plans specific to its Hosted Environment and shall include failover configurations.

5 **ATTESTATIONS OF COMPLIANCE.** Upon Customer's reasonable written request, Verint shall provide an attestation of compliance to the terms in this Schedule which may include Verint's applicable Industry Standard security assessment questionnaire responses which may be delivered through Verint's authorized partners. Such requests shall be made in writing through the Account Executive assigned to Customer unless otherwise specified by Verint.