OnProcess

Supplier Guidelines

Information is a critical business asset and OnProcess' ability to manage, control, and protect this asset is critical to OnProcess' interests. "Information" shall be considered and defined in the broadest sense to include, but not be limited to, any research, intellectual property, personally identifiable information, business and product development, test and evaluation data, sales, marketing and business plans, customer and supplier information, supply chain, distribution, finance, human resources, consulting, partnerships, contracts, mergers and acquisitions, and any other information related or pertaining to OnProcess, or OnProcess' employees, clients, subcontractors, and/or suppliers that would reasonably be considered "confidential" as such term or its equivalent is described in the underlying agreement. A subset of Information is Personally Identifiable Information.

"Personally Identifiable Information" or "PII" is any information provided by OnProcess or a OnProcess client, or collected by Supplier in connection with Supplier's relationship with OnProcess (i) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, (ii) from which identification or contact information of an individual person can be derived, or (iii) that constitutes Protected Health Information (PHI) as that term is defined in the U.S. Health Insurance Portability and Accountability Act. PII includes, but is not limited to: name, address, phone number, fax number, email address, social security number or other government-issued identifier, credit card information and any health-related information. Additionally, to the extent any other information (such as, but not necessarily limited to, a personal profile, unique identifier, biometric information, and/or IP address) is associated or combined with PII, then such information also will be considered PII.

The Guidelines are designed to provide a uniform minimum compliant standard for every OnProcess Supplier with respect to its protection of Information worldwide. OnProcess recognizes that certain laws may require stricter standards than those described in these Guidelines. In those situations, Supplier must handle Information in accordance with all applicable laws, including any stricter standards than those described in these Guidelines. Where applicable law provides a lower level of protection of Information than that established by these Guidelines, the requirements of the Guidelines shall apply.

Data Protection

Supplier shall at all times comply with all obligations under applicable data protection legislation in relation to all information that is processed by it or to which it has access in the course of performing its obligations under the underlying agreement, including by (a) maintaining a valid and up to date registration or notification under the data protection legislation and (b) complying with all data protection legislation applicable to cross border data flows of information and required security measures for information. Supplier shall maintain a comprehensive data security program, which shall include appropriate technical, organizational and security measures against the destruction, loss, unauthorized access or alteration of OnProcess information in the possession of Supplier, and which shall be (i) no less rigorous than those maintained by Supplier for its own information of a similar nature, and (ii) no less rigorous than accepted security standards in the industry. Supplier shall not use OnProcess information for any purpose other than the fulfillment of Supplier's obligations under the underlying agreement. Supplier shall not process, transfer, disclose, transmit or disseminate information without the approval of OnProcess and only in accordance with OnProcess' instructions. Supplier shall take appropriate action to ensure the reliability of any personnel who have access to information and to cause its personnel having access to information to be advised of the terms of these Guidelines and trained regarding their handling of such information. Supplier shall be responsible for any failure of its personnel to comply with the obligations of Supplier as set forth in these Guidelines.

If Supplier has knowledge of any unauthorized disclosure of or access to OnProcess information, Supplier shall notify OnProcess of such breach or potential breach by email to securityadvisory@onprocess.com within twenty-four (24) hours of learning thereof. If the unauthorized disclosure relates to OnProcess information that is in the possession of or otherwise within Supplier's areas of control, Supplier shall take the following additional actions: (A) investigate (with OnProcess' participation if so desired by OnProcess) such breach or potential breach, (B) perform a root cause analysis and prepare a corrective action plan, (C) provide written reports of its findings and proposed actions to OnProcess for review and approval, and (D) to the extent such breach or potential breach is within Supplier's areas of control, remediate such breach or potential breach of security and take commercially reasonable actions to prevent its recurrence. Supplier will cooperate with OnProcess

with respect to any such unauthorized disclosure in the manner reasonably requested by OnProcess. Such cooperation will include without limitation: (i) providing OnProcess access to applicable Supplier records and facilities so long as such access does not breach the confidentiality obligations of Supplier to third parties not involved in provision of the Services under this Agreement; and (ii) providing OnProcess with all relevant data and reports. Supplier shall obtain prior written approval from OnProcess regarding any notifications to impacted individuals, government agencies, or media. If any unauthorized disclosure of or access to OnProcess information is attributable to the negligent act or omission of Supplier or its personnel, or a breach by Supplier or its personnel of Supplier's obligations under the underlying agreement, Supplier shall bear the costs incurred in complying with its legal obligations relating to such breach.

Supplier agrees to cooperate with OnProcess in its privacy compliance efforts, including executing a Data Processing Agreement or similar agreement as reasonably requested by OnProcess.

Access to Information Systems

Access to OnProcess' information systems (the "Information Systems") is granted solely to perform the services under the underlying agreement, and is limited to those specific Information Systems, time periods and personnel as are separately agreed to by OnProcess and Supplier. OnProcess may require Supplier's employees, subcontractors or agents to sign individual agreements prior to access to any Information Systems. Use of the Information Systems during other time periods or by individuals not authorized is expressly prohibited. Access is subject to OnProcess' business control and information protection policies, standards and guidelines as may be modified from time to time. Use of any other Information Systems is expressly prohibited. This prohibition applies even when an Information System that Supplier is authorized to access serves as a gateway to other Information Systems outside Supplier's scope of authorization. Supplier agrees to access Information Systems only from specific locations approved for access by OnProcess. OnProcess will designate the specific network connections to be used to access Information Systems.

Use of Information

Supplier must collect, use, or access Information only in compliance with applicable law, the underlying agreement, and these Guidelines. Supplier shall make its employees aware of the key elements of the Guidelines to ensure they understand their personal responsibilities. Supplier shall educate/train its staff in how to implement the Guidelines. Supplier may substitute its own privacy and security training with training on the Guidelines if such training is comprehensive and materially addresses the requirements within the Guidelines. Supplier shall implement procedures to confirm that the services being performed for OnProcess are compliant with the Guidelines.

Use of PII

To the extent Supplier is afforded access to or handles any PII, use of PII shall be governed by the following requirements.

Supplier shall limit the collection and access of PII to that which is strictly necessary to perform services for OnProcess or to fulfill any legal requirements. Prior to collecting or processing PII, (i) Supplier shall identify to OnProcess the PII it intends to collect and the proposed use for such Information, and (ii) Supplier shall get written approval from OnProcess (execution of a work order or its equivalent that explicitly contemplates the collecting or processing of PII constitutes written approval). If services being performed for OnProcess involve the collection of PII directly from individuals, such as through a webpage, Supplier must provide a clear and conspicuous notice regarding what PII is being collected and its intended use.

Supplier shall appoint an individual to coordinate the privacy and security arrangements in relation to the work being performed for OnProcess ("Privacy Coordinator"). The Privacy Coordinator will have responsibility for verifying that Supplier complies with the Privacy and Security portion of the Guidelines.

Supplier shall maintain PII in strict confidence in accordance with the confidentiality obligations entered into with OnProcess.

Supplier shall not share PII in its possession or that it collects with any third parties for any reason except as necessary to carry out the services being performed for OnProcess and as pre-approved in writing by OnProcess.

If served a court order compelling disclosure of PII or with notice of proceedings for such an order, Supplier shall oppose the order, notify OnProcess of such order or notice, and provide OnProcess the opportunity to intervene before filing a response to the order unless otherwise prohibited by law.

Supplier shall take all reasonable administrative, technical, and physical steps to protect PII in Supplier's possession from unauthorized use, access, disclosure, alteration or destruction. Supplier's security measures shall include access controls, encryption or other means, where appropriate.

Supplier shall utilize a formal and documented internal process for incident reporting and incident response related to actual or suspected unauthorized disclosures of PII. Such process shall meet corresponding industry standards for incident reporting and response.

Supplier shall immediately notify OnProcess of any known or suspected incident that has, could reasonably be expected to have, or will later result in the unauthorized use, access, disclosure, alteration or destruction of PII. Supplier agrees to fully cooperate with OnProcess in the investigation of any such incident, and in the event that an incident involves PII in Supplier's or its Subcontractor's custody, Supplier will, in addition to any other remedies permitted by agreement between the parties, make best efforts to (i) eliminate the risk of continued unauthorized use, access, disclosure, alteration or destruction of PII, and (ii) mitigate the damages from the unauthorized use, access disclosure, alteration, or destruction of PII.

Supplier shall explore and, where possible, implement measures designed to minimize further use of PII (e.g., assigning identification or account numbers that do not correspond with Social Security numbers) for future performance of services.

Supplier shall destroy all PII in a manner that renders it unreadable (e.g., shredding, etc.) when it is no longer needed for the performance of services for OnProcess unless otherwise instructed by OnProcess.

Upon request, Supplier shall provide a diagram detailing how PII is received, stored, processed and transmitted (as applicable) while in Supplier's custody.

Destruction of PII

Supplier shall, within five business days of termination of any applicable agreement entered into between Supplier and OnProcess, or upon request by OnProcess either:

Provide OnProcess with all documents and materials containing PII, or;

Destroy all such documents and materials and provide OnProcess with a certificate of destruction signed by an officer of Supplier.

Subcontracting

If permitted by agreement to utilize a third-party to perform any services for or on behalf of OnProcess ("Subcontractor"), Supplier shall require the Subcontractor to adhere to these Guidelines. If requested, the Supplier must certify Subcontractor's compliance with the Guidelines to OnProcess in writing before using such Subcontractor to perform any services on OnProcess' behalf.

PCI

To the extent Supplier stores, transmits, or processes any Cardholder Data (as such term is defined by the PCI DSS) in providing services for or on behalf of OnProcess, Supplier shall comply with the Payment Card Industry Data Security Standards (PCI DSS) and/or the Payment Application Data Security Standards (PA DSS) as applicable. To the extent the services being performed for OnProcess involves either PCI DSS or PA DSS, Supplier acknowledges that the security of cardholder data is its responsibility while such data is in Supplier's custody or control. Upon request, Supplier shall provide certification of its compliance with either PCI DSS or PA DSS.

Audit

If Supplier handles any PII for or on behalf of OnProcess, Supplier shall conduct an audit, at no cost to OnProcess, on at least an annual basis to evaluate the security of PII in its possession and to verify that the terms of these Guidelines are being followed. The results of such audit shall be made available to OnProcess upon completion of the audit. Supplier will not be required to share any confidential information of third parties or information unrelated to the services being performed for OnProcess contained within such audit results.

In the event of an unauthorized disclosure or use of PII by Supplier, Supplier agrees to hire a third-party of OnProcess' choosing (provided such third-party is not a direct competitor of Supplier) to conduct an additional audit of the Supplier-OnProcess environment against the requirements of the Guidelines.

OnProcess reserves the right, at its own cost, to audit Supplier's information security practices against compliance with these Guidelines on reasonable notice.

For all audits, Supplier agrees to remediate any shortcomings in the audit findings at Supplier's exclusive expense and verify such remediation to OnProcess upon completion.

Equipment and Information Security

To safeguard against unauthorized access to Information by third parties outside OnProcess, all electronic Information containing PII held by Supplier shall be maintained on systems that are protected by secure network architectures that contain firewalls, regularly monitored intrusion detection devices, and strong encryption. The servers holding Information shall be "backed-up" (i.e., the data are recorded on separate media) on a regular basis to avoid the consequences of any inadvertent erasure or destruction of Information, and such back up media shall also be encrypted. The servers shall be located in facilities with comprehensive security and fire detection and response systems.

Company Property and Resources

OnProcess property and resources are highly valuable. OnProcess property may not be taken, sold, loaned, given away, licensed, assigned, damaged or otherwise disposed of regardless of its condition or value, unless Supplier has specific written authorization from OnProcess to do so.

Background Checks

Supplier personnel shall not perform any work for OnProcess if the appropriate pre-placement screening (as detailed below) discloses information that Supplier would reasonably conclude would make the individual unacceptable for placement at OnProcess ("Unacceptable"). In addition to any other requirements set forth in the Agreement, the following are specific requirements for pre-placement screenings on Supplier personnel performing services for OnProcess based upon the type of access to OnProcess assets the personnel will have:

All Supplier personnel providing services for or on behalf of OnProcess must at a minimum have, to the extent permitted by law: (1) a national-level (i.e., not limited to local geography) criminal background check, and (2) checks performed against the terrorist watch, "Specially Designated National" or "Blocked Person" lists under U.S. Executive Order 13224, published by the U.S. Department of the Treasury's Office of Foreign Assets Control. The parties agree that Supplier personnel having either (i) been convicted of any felony or a misdemeanor involving theft or dishonesty, or (ii) been flagged under the "Specially Designated National" or "Blocked Person" list are considered Unacceptable for placement on OnProcess services.

All Supplier personnel providing services for or on behalf of OnProcess that may have access to multiple pieces of PII (i.e., personnel who have access to spreadsheets containing PII, access to databases storing or processing PII, network administrative access, access to multiple personnel or financial files, etc.) ("PII Personnel") must have, to the extent permitted by law (a) the pre-placement screenings identified in the above bullet, and (b) a drug screen for illegal use of controlled substances. In addition to the practices mutually considered Unacceptable for placement on OnProcess services for non-PII Personnel, any drug screen results indicative of illegal use of a controlled substance will be considered "Unacceptable" by the parties for PII Personnel. For clarity, Supplier personnel who have incidental

contact with PII or contact with very low volume of singular pieces of PII (single piece of contact information, individual employment records, etc.) are not considered PII Personnel, but those personnel who have the potential to access to PII but never do are considered PII Personnel.

Supplier shall conduct all pre-placement screenings in accordance with applicable law.

Confidential Information and Privacy

OnProcess values and protects Information, including information about its customers, employees, operations, finances and business plans. Supplier is required to preserve OnProcess Information as confidential and in accordance with confidentiality agreements and proprietary/confidential legends. Any disclosure of OnProcess Information is prohibited. This includes inadvertent disclosures, which means that Supplier shall not have discussions involving OnProcess Information in public areas where discussions could be easily intercepted or overheard. Supplier may use OnProcess Information solely for the purpose for which it is provided under the agreement or in compliance with the confidential/proprietary legend and must not make independent use of OnProcess Information.

Criminal Activity

Supplier shall immediately remove individuals from the services being performed for OnProcess and from OnProcess property, if OnProcess or Supplier becomes aware of criminal activity by such individual.
Supplier shall comply with all applicable laws when removing any individual from OnProcess premises.

Supplier must inform its OnProcess business contacts immediately after becoming aware of criminal activity information that would suggest a threat of physical harm to OnProcess property or employees.

Specific Security Controls

Supplier must not store any PII on a mobile device (including laptops, PDAs, thumb drives, etc.) without explicit and documented approval from OnProcess Information Security. If such written approval is granted, all such PII on mobile devices must be encrypted using industry standard encryption methods.

Supplier shall not send unencrypted PII over public networks.

Supplier may not remotely access the OnProcess network without documented approval from OnProcess Information Security.

If Supplier connects to OnProcess networks in any manner, Supplier must use automated and up-to-date anti-virus definitions and industry standard anti-virus software on all Supplier devices/networks connecting to the OnProcess network.