HCL VENDOR SECURITY REQUIREMENTS

This document describes HCL's information security, business continuity, privacy practices, standards and its program for assessing the information security and business continuity practices of its vendors and partners. It contains confidential information of HCL and is provided pursuant to a nondisclosure agreement or vendor services agreement. The recipient may not distribute or disseminate this document internally except on a need-to-know basis or externally without prior written permission of HCL.

This Vendor Security Requirements Document is intended to inform Vendor of the information security, business continuity and privacy practices that HCL expects of its Vendor and to which Vendor will be held responsible. It is to be used in the provision of services to HCL only. Vendor should implement these requirements in accordance with industry best practices and their corporate security policies (ex: evaluating them in a non-operational environment if prudent) in consultation with a HCL representative. In no event will HCL be liable for vendor's inability to access information or for any damage vendor suffers, including, but not limited to, destruction of data or damage to vendor's equipment, whether such damage is direct, incidental or consequential, and whether caused by mistake, omission, interruption, deletion of files or messages, errors, defects, delays in operation or transmission, failure of equipment or performance, negligence or otherwise. To the extent any inconsistencies exist between this Vendor Security Requirements Document and the negotiated terms in the written agreement between the Vendor and HCL, the language in such written agreement shall prevail.

Vendor who provide services that may be subject to local, national, regional regulatory and statutory requirements that affect compliance with certain of the HCL Standards set forth in this Vendor Security Requirements Document. In the event of a conflict between the requirements in the Vendor Security Requirements Document and any regulatory or statutory requirement applicable to a Vendor, the applicable local, national or regional regulatory or statutory requirement shall prevail. If such a conflict exists, the Vendor shall inform HCL of the underlying regulatory requirements which affect compliance and propose mitigating controls to provide an equivalent level of information security, business continuity or privacy.

Table of Contents

Overview of Vendor Security Requirements

HCL has a responsibility to protect its restricted and confidential information from unauthorized access or disclosure. For this HCL implements internal information security, business continuity and privacy standards to ensure that such restricted and confidential information is protected and that the services provided by HCL are continuously available. To ensure HCL's compliance with internal standards and regulatory requirements relating to information security and business continuity, HCL requires that its Vendors adhere to HCL Standards. In turn, to the extent a Vendor delegates or subcontracts to a Vendor any portion of Vendor's obligations under its agreement with HCL, or, engages a Vendor to provide services directly or indirectly to HCL, the Vendor shall require such Vendor to implement and administer an information protection program and plan that complies with HCL Standards. HCL is committed to working with its Vendor to help Vendor meet compliance requirements relating to HCL Standards. This document sets forth an overview of the HCL Standards with which Vendors are expected to comply and with which compliance may be evaluated through the Vendor Risk Assessment Program. The extent of the applicability of such HCL Standards to a particular Vendor will vary depending on the type of service and products provided by such Vendor to HCL.

Definitions

"Agreement" is the MSA or other master agreement to which this VSR Document has been appended
"Availability" is the property of being accessible and usable upon demand by an authorized entity
"Confidentiality" is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes
"Customer Data" means all data and information, including the Customer IP and Covered Information, (a) submitted to Vendor or Vendor Agents by or on behalf of any Service Recipient, (b) obtained, developed or produced by Vendor or Vendor Agents in connection with the Agreement or (c) to which Vendor or Vendor Agents have access in connection with the provision of the Services.
"Effective Date" is the date on which the Agreement becomes effective
"Sub-contractor" is defined as any entity or individual providing services to the Vendor that has a direct or indirect relation to the Services delivered to HCL.
"HCL Information" is information and data received by the Vendor from HCL as part of the Agreement and governed by the VSR Document, including Personal Data and/or Customer Data, as well as any new

data created by the Vendor from the said information and data (including aggregated or anonymized data)

“Integrity” is the property of safeguarding the accuracy and completeness of assets

“VSR Document” is this document entitled ‘HCL Vendor Security Requirements’ and appended to the Agreement

“Personal Data” has the meaning given in the EU Data Protection Directive, but data is also Personal Data for the purposes of the Agreement if it is any information (a) that, either individually or when combined with other information, can be used to identify a specific individual or derive information specific to a particular individual, and any information or data related to the current, past or potential employees or customers of Customer or its Affiliates, and (b) covered by Privacy Laws, including the following: (i) a first name and last name; (ii) a home or other physical address, including street name and name of city or town; (iii) an email address or other name, that reveals an individual's email address; (iv) a telephone number; (v) a Social Security number; (vi) credit or debit card information; (vii) checking account information, account number and check number; (viii) a driver's license, military or state identification number; (ix) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; (x) human resources information, such as benefits plan information, member number, salary information, performance history, health history, and similar information; (xi) financial or transactional information; (xii) employee ID number; (xiii) government passport number or alien registration number, or (xiv) any other information that is identifiable to or identifies an individual, whether combined with any of (i) through (xiv) above.

“Personal Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” in 45 C.F.R. § 160.103, limited to the information created or received by Vendor from or on behalf of HCL or HCL’s Customer.

“PII” means any information which identifies or is capable of identifying an individual, or is otherwise defined as “personal information” or “personal data” by applicable Laws including: (a) an individual’s name, address, phone number, e-mail address, initials, social security number, ID number or credit card information; and (b) information, data and materials, including demographic, medical and financial information, that relate to the past, present, or future physical or mental health or condition of an individual or the provision of health care to an individual.

“Privacy Laws” means Laws that relate to the confidentiality, collection, use, handling, processing, encryption, privacy, security, protection, loss, disclosure, storage, transmission, transfer (including cross-border data flows) or free movement, breach notification, and unauthorized access of personal data or personally identifiable information, including the EU Data Protection Legislation.

“Security Incident” is an actual, potential, or attempted security breach or possession, use, knowledge, destruction, loss, alteration, disclosure or theft of, or unauthorized access to, HCL Confidential Information, including Personal Data and/or Customer Data, in violation of this VSR Document or applicable law, or explicit or implied security policy ,or standard which may or may not result in loss of HCL Information, Personal Data, and/or Customer Data and/or adverse effects and disruption of service.

“Services” are the data processing activities and other procedures carried-out by the Vendor on HCL Information in terms of the Agreement or as otherwise instructed or directed by HCL

“Vendor” is anyone who provides goods or services to HCL as contemplated in the Agreement

"Work Results" means any inventions, methods, techniques, improvements, software designs, computer programs, strategies, data and other works of authorship developed by Vendor while providing Services under the Agreement.

1 Right to Audit

1.1. HCL reserves the right to perform a risk assessment if required and appropriate, yet not without prior written notification to the Vendor, and without creating a business disturbance for the Vendor. Assessment may be performed by HCL and/or by HCL nominated third party and the information obtained during the assessment shall be treated with confidentiality within HCL.

2 Incident Notification

2.1. Vendor will promptly inform the authorised HCL representative of any Security Incident or attempt thereof involving HCL Information being processed by the Vendor or any subcontractor, as well as breach of any applicable privacy and data protection laws, within 12 hours of the breach being initially discovered. Immediately following the Vendor's notification to HCL of the breach, the Vendor and HCL shall coordinate and cooperate with each other to investigate such Security Incident. The Vendor shall provide all assistance requested by HCL in investigating, preventing, and mitigating the effects of such Security Incident. The cost of such investigation shall be solely attributable to and borne entirely by the Vendor alone, without prejudice to other rights and remedies available with HCL under the Agreement towards such Security Incident; and

2.2. Notification of Security Breaches shall be sent via e-mail to Infosecincidents@hcl.com, vrm@hcl.com and to Vendor's primary business contact within HCL.

2.3. Vendor shall establish a process for dealing with incidents that require forensic investigations

2.4. Vendor shall take reasonable steps to immediately remedy any Security Breach and prevent any further Security Breach at Vendor's expense in accordance with applicable privacy rights, laws, regulations and standards.

3 Sub-Contractor engagement

3.1 The Vendor shall not sub-contract any of its services that it is obligated to perform under the agreement without prior written consent of HCL. Where the Vendor sub-contracts its obligations with the consent of HCL, it shall do so only by way of written agreement with the sub-contractor(s) which imposes the same obligations on the sub-contractor(s) as are imposed on the Vendor under the Agreement. Where the sub-contractor(s) fails to fulfil its obligations under such written agreement, the Vendor shall remain fully liable to HCL for the performance of the sub-contractor's obligations under such agreement.

4 Access Control

4.1. Access to the application and associated information must be restricted to authorized individuals, enforced accordingly, ensure that only authorized individuals gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorized users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

4.2. Quarterly access review process may be established.

4.3. Vendor shall ensure the access rights of Service employees are removed upon termination or when they are moved out of HCL engagement or when their roles have changed.

5 General Data Protection

5.1. HCL will retain unrestricted, absolute and unlimited rights and ownership to HCL Information. Vendor shall have no ownership rights in Customer Data, Personal Data, PII, or PHI.

5.2. The Vendor shall provide full and up-to-date copies of HCL Information hosted on the Vendor's infrastructure at no additional cost within one (1) working day of HCL's request for the same or within the timeframe specified otherwise. This clause shall also apply to HCL Information, PII, Customer Data, and Personal Data not destroyed / disposed-off upon termination of the Agreement and held / retained by the Vendor in terms of clause 5.15 below.

5.3. The vendor shall appoint or establish a single point of contact to handle and respond to all Privacy and Data Protection queries of HCL, confirm compliance with all privacy and data protection laws, rules, regulations, orders, conventions and ordinances applicable to HCL and the Vendor, and to confirm that data processing policies and procedures required to be followed and adhered to by the Vendor under the Agreement have been implemented and maintained.

5.4. HCL Information shall only be used for the purpose(s) set out in the Agreement and shall not be processed further, disclosed or made accessible to any Vendor, without the explicit prior written consent of HCL.

5.5. The Vendor on receiving any lawful access request to HCL Information by way of order of a court or subpoena, or by a law enforcement agency, shall inform HCL of any such request within two (2) working days of receiving such request. The Vendor shall act as an HCL representative during all privacy related proceedings or enquiries received from the government regulator(s) in connection with HCL Information being processed by the Vendor. The Vendor, wherever necessary, will notify the regulator of the nature of its data processing and will, at all times, ensure compliance with all privacy and data protection laws applicable to HCL under the Agreement or the larger agreement.

5.6. The requirements of this VSR Document and any security requirements in the Agreement must be imposed on any Vendor/sub-contractor(s) providing services to the Vendor in case the Vendor chooses to use their services to fulfil its obligations under the Agreement. Vendor will provide to HCL evidence in the form of signed legal documentation showing this VSR Document being imposed as a requirement on any subcontractors. Vendor

acknowledges that it will remain responsible vis-à-vis HCL and the data subjects of HCL Information for any breach under the Agreement caused by actions or inactions of its sub-contractor(s).

5.7. Vendor agrees to take all the actions as may be required to respond to any request for access, change, correction, or choice modification to HCL Information, made by or through HCL, or made pursuant to procedures established by HCL, in a manner which will result in completion of the action in a period (inclusive of any time required by Vendor's subsequent sub-vendors) no longer than: (1) thirty (30) days; or (2) such period that may be imposed on HCL as a matter of applicable law; whichever is shorter. Any access request(s) made to the Vendor by the data subjects of HCL Information, will be forwarded to HCL not later than two (2) days of receiving such request, and the Vendor will follow any instructions provided by HCL for responding to such request(s).

5.8. Vendor shall not transfer or permit the transfer by its sub-contractor(s) of any HCL Information to a location, including a cloud storage location, for processing or for data backup or for any other such purposes, other than to a location as specifically provided and mentioned in the Agreement or with explicit written prior consent of HCL.

5.9. Vendor shall establish and maintain safeguards and take all reasonably necessary technical, organizational and physical precautions to protect HCL Information against Security Incident including but not limited to destruction, loss, theft or unauthorized alteration, access, disclosure, erasure, copying, use or manipulation of HCL Information while in the possession or under the control of the Vendor and its sub-contractor(s).

5.10. Vendor shall limit disclosure of or access to HCL Information only to its employees who have a legitimate business need to access this information in terms of the Agreement, and who have received proper training and instruction as to the requirements of the Agreement or any applicable privacy and data protection laws in force. Vendor accepts full liability for any breach under the Agreement by any of its employees and/or its sub-contractor(s), with respect to data obligations under the Agreement.

5.11. The Vendor shall reimburse HCL for all actual costs incurred in providing data subjects of HCL Information affected by any Security Incident with notice of such breach and/or incident, as well as for other costs that HCL in its sole discretion may determine reasonable and deem appropriate to protect such affected data subjects, in light of the risks posed by the Security Incident.

5.12. The Vendor agrees to provide HCL with such information and access to its premises (upon a notice of three (3) working days) for audit purposes as HCL may reasonably require to ensure itself that the Vendor and/or its sub-contractors are complying with the obligations referred to in the Agreement and to determine if HCL Information is being processed in an appropriate manner and the steps to protect the personal data as agreed are being fulfilled. HCL is hereby vested with absolute rights to audit the Vendor and/or its sub-contractor(s) immediately in the event of a Security Incident wherein the scope of such audit shall be limited to the scope of the Security Incident as determined in its sole discretion by HCL.

5.13. Vendor agrees to defend, indemnify and hold HCL harmless from any liability, claims, damages, fines, penalties, costs, demands and expenses (including costs of defence,

settlement and reasonable legal fees), arising from or related to any breach of this VSR Document or part thereof by the Vendor or its sub-contractor(s). Vendor will not settle any dispute or agree to any settlement without the prior written consent of HCL. HCL reserves the right to engage its own counsel and to actively participate in all settlement and other related proceedings and litigation as it in its sole judgment determines necessary or desirable.

5.14. The Vendor must obtain and maintain cyber liability insurance covering claims based on violation of any applicable privacy rule(s), privacy and data protection laws, or regulation concerning the privacy of HCL Information and claims based on obligations pursuant to this VSR Document with coverage of not less than one million US Dollars (USD 1,000,000) per occurrence.

5.15. In the event of termination of the Agreement, HCL at its sole discretion may instruct and direct the Vendor to either return to HCL or erase, HCL Information or any copies of part thereof, from the Vendor's information systems (electronic and/or physical form) and from that of its sub-contractor(s). HCL may also direct the Vendor to destroy HCL Information and/or equipment in terms of clause 10.2 below or to hold / retain the said HCL Information and/or equipment, till HCL's further direction(s).

5.16. The Vendor shall, to the extent possible, enumerate the type and elements of HCL Information collected or processed and attach to the Agreement.

5.17. The Vendor shall, whenever applicable, enter into a separate Data Transfer Agreement with HCL.

5.18. Vendor discloses Personal Data to HCL solely for: (i) a valid business purpose; and (ii) Vendor to perform the Services.

5.19. Both parties are prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing the Personal Data outside of the Agreement between Vendor and HCL.

5.20 Each party shall notify the other party if the former party determines it can no longer abide by the rights and obligations associated with the information it is processing on the other party's behalf; or if, in it's opinion, an instruction to process personal data is in violation of a privacy law.

6 System Security requirements

6.1. Vendor shall implement administrative, physical and technical safeguards to protect HCL's or its customer's information that are no less rigorous than accepted industry practices (such as ISO/IEC 27001:2013 – Information Security Management Systems – Requirements and ISO-IEC 27002:2013 – Code of Practice for International Security Management, The Control Objectives for Information and related Technology (COBIT) standards [or] other applicable industry standards for information security), and shall ensure that all such safeguards, including the manner in which the information is collected, accessed, used,

stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of the Agreement.

7 Business Continuity Management (BCM)

7.1. Business Continuity Plan (BCP) and IT Disaster Recovery Plan (DRP) must be developed, supported by contingency arrangements, and tested periodically. BCP and DRP, including BCP test results shall, upon request in writing, wherever feasible, be shared with HCL.

8 Cloud

8.1. When HCL information is co-located with non-HCL data, (e.g., virtual servers, cloud solutions, etc.) the non-HCL data must be logically separated from the PII and/or HCL information.

8.2 Before relocating the physical storage location of PII and/or Customer Data and Personal Data HCL information to a country different from the ones documented in the statement of work or contract, HCL's consent must be obtained in advance so that potential implications for privacy can be addressed.

8.3. Cross Border Transfer: Verify that the correct data transfer contracts are in place prior to transferring the information, if personal information is to be transferred to any country other than the country where is collected.

8.4. Cloud solutions need to be able to protect the data, maintain both data quality and data integrity.

8.5. Cloud–sourced solutions must adhere to standard information security principles and applicable government regulations, laws, or directives. Vendors must be vetted on an individual basis including any indemnification considerations and sub-contractors.

8.6. HCL or its customer data shall be encrypted both while at transit and at rest.

9 Intellectual Property Rights

9.1. Both Parties agree and acknowledge that performance of the Agreement, including the Statements of Work, may result in the discovery, creation or development of Work Results as well as usage of any Pre-existing IP of either Party. Vendor agrees to deliver to HCL the Work Results promptly.

9.2. Vendor agrees and acknowledges that all Intellectual Property Rights, title and interests in and to the Work Results shall fully vest in HCL on the creation of the same. To this end, Vendor fully and effectively assigns and transfers, and will ensure that each Vendor Employee will fully and effectively assign and transfer, to HCL all rights, title and interests in and to the Work Results. In particular, but without prejudice to the generality of the foregoing, all copyright and patent rights in and to the Work Results including but not limited to the right of transfer, sale, modification, sub-leasing and licensing of such Work Results to third parties shall vest in, and be assigned and transferred to HCL. All Pre-existing IP owned by each Party shall remain vested in that Party with full ownership rights therein. Unless otherwise specifically agreed upon in a Statement of Work, neither Party shall get any rights in the Pre-existing IP of the other Party. Vendor shall not incorporate any of its

Pre-Existing IP or any third party IP in any Work Results without requiring HCL's prior written consent. Further, HCL acknowledges that Vendor provides consulting, implementation, maintenance and support services to its other clients/customers and agrees that nothing in the Agreement shall be deemed or construed to prevent Vendor from conducting such business by using Pre-existing IP of Vendor, unless otherwise stated explicitly in the Statement of Work. Vendor agrees to grant to HCL, for its benefit and for the benefit of its Affiliates, Clients (including their Affiliates) and agents a royalty-free, fully paid–up, non–exclusive, transferable, irrevocable, perpetual license to the extent reasonably necessary to enjoy the benefit of the Services and/or the Work Results. Vendor hereby irrevocably and unconditionally waives all moral rights and all other relevant rights as required in connection the Intellectual Property Rights that is comprised in the Work Results to the extent permitted by applicable law.

9.3. Vendor hereby undertakes to fully indemnify and keep fully indemnified HCL against any liability for loss, claims, demands, expenses and legal fees directly incurred in this connection arising out of any claim or losses or damages incurred by the Vendor arising out of or in relation to a claim that the Services, Work Results or any part thereof constitutes an infringement or alleged infringement of the Intellectual Property Rights of a third party.

9.4. In the event that the Services or any part thereof are held to constitute an infringement of any rights of third party(ies), Vendor shall at its expense and on receipt of written request from HCL either:

(a) procure the right to continue providing the Services or infringing part thereof within a reasonable time; or

(b) modify the provision of the Services or infringing part thereof in agreement with HCL so that they are non-infringing and satisfy the specifications of the relevant Statement of Work.

10 Data Retention and Return

10.1. Vendor shall implement controls to protect records and information assets in accordance with statutory, regulatory, contractual and HCL business requirements. All related information assets shall be retained till necessary to support the services provided to HCL or its customer or as mandated by relevant regulations.

10.2. Vendor shall return, destroy or dispose all information after the relevant timeframe in a secure manner using industry standard data wiping process. Upon termination of the Agreement, Vendor shall confirm, within 30 days of termination of the contract about the return of all information assets to HCL or about securely wiping off HCL's or its customer's information. Any sensitive HCL information or its customer' shall be destroyed in such a manner that it cannot be retrieved or restored.

Processing of Personal Data

The following terms are also incorporated into the HCL Purchase Order terms / Agreement governing delivery of goods/service by the Vendor to HCL and Vendor agrees to comply with the same:

1. The data processing must be undertaken by the Vendor only in accordance with written documented instructions.
2. The Vendor's personnel must be subject to obligations of confidentiality and shall be trained with respect to privacy and data protection requirements. To the extent that Vendor's personnel process personal data, they shall have specific training on the requirements of the applicable data protection law. Any resource not already trained shall be trained within 90 days of the signing of this Agreement.
3. The Vendor must cooperate with HCL in establishing appropriate technical and organizational measures necessary to protect the personal data.
4. The Vendor must keep the personal data it is processing secure which includes, but is not limited to, the use of appropriate encryption technology, security, integrity, availability, and anonymization.
5. The Vendor must not subcontract any part of the processing of personal data without HCL's written consent and the same data protection obligations must be flowed down into the terms of the subcontract including, but not limited to, obligations to implement appropriate technical and organizational measures to ensure the security of the personal data.
6. The Vendor must assist with the implementation of appropriate technical and organizational measures regarding data subjects' access rights.
7. As soon as possible, but in no event more than 24 hours from discovery, Vendor must: (i) ensure the security of processing; (ii) provide notifications to HCL of any personal data breach; (iii) assist HCL in ensuring compliance with data breach notification obligations; (iv) assist with the preparation of any data protection impact assessment; (v) assist with any prior consultations that HCL has with any supervisory authority; and provide formal written communication including actions taken to mitigate, if it was possible to do so.
8. At the end of the agreement, Vendor must delete or return any personal data to HCL unless the Vendor is required to keep a copy in order to comply with applicable law.
9. The Vendor must provide HCL with all information that HCL requires in order to demonstrate Vendor's compliance with the agreement.
10. The Vendor must cooperate with HCL and HCL's Customer in relation to any data protection audit (which also includes any inspections) relating to personal data the Vendor is processing for HCL.
11. Vendor hereby warrants that it is compliant with applicable data protection laws. The Vendor must inform HCL if it suspects potential violation of any applicable data protection law.
12. The Data Transfer Agreement must clearly set out: (i) the subject matter of the agreement; (ii) the duration; (iii) the nature and purpose of the processing; (iv) the type of personal data to be processed; and (v) the categories of the data subjects.