DATA PROTECTION AGREEMENT

Dell and Provider have entered into a Provider Agreement under which Provider may process Dell Data in connection with the provision of Solutions. This Data Protection Agreement ("**DPA**") governs Provider's processing of Dell Data and shall form part of and be incorporated by reference into the Provider Agreement. At all times during the term of the Provider Agreement, or after the term if Provider retains access to Dell Data, Provider shall, and shall cause its Representatives to, comply with this DPA. In the event of a conflict between the DPA, the NDA and/or the Provider Agreement, this DPA shall prevail.

1. **DEFINITIONS.** Terms not defined herein have the meanings set forth in the Provider Agreement.

1.1 "**Applicable Law**" means any and all applicable laws, statutes, and ordinances, rules, regulations, directives, edicts and similar governmental requirements of all international, federal, provincial, state, county, city, and borough departments, bureaus, boards, agencies, offices, commissions and other subdivisions thereof, or any other governmental, public, or quasi-public authority.

1.2 "**Controller**" means an entity which, alone or jointly with others, determines the purposes and means of the processing of the Personal Data.

1.3 "**Data Breach"** means any accidental, unlawful, or unauthorized destruction, alteration, disclosure, misuse, loss, theft, access, copying, use, modification, disposal, compromise, or access to Dell Data or any act or omission that compromises or undermines the physical, technical, or organizational safeguards put in place by Provider in processing Dell Data or otherwise providing Solutions.

1.4 "**Dell Data**" means any and all data provided by Dell, its customers, authorized agents and/or subcontractors to Provider, or otherwise processed by Provider in connection with the provision of Solutions, including (a) all non-public information and data provided to or accessed by Provider through Dell's network, or provided to or accessed by Provider for hosting or outsourcing services, (b) Highly Restricted Data, (c) Personal Data and/or (d) User Tracking Data.

1.5 "**EEA**" mean the Member States of the European Union plus Norway, Iceland and Liechtenstein.

1.6 "**GDPR**" means the General Data Protection Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as amended or superseded from time to time.

1.7 "**Highly Restricted Data**" means Social Security or other government-issued identification numbers, medical or health information, account security information, individual financial account information, credit/debit/gift or other payment card information, account passwords, individual credit and income information, intellectual property, proprietary business models, pricing, customer infrastructure/system information or data flows and sensitive personal data as defined under Privacy Laws (including the GDPR).

1.8 "**Including**" means including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and "include" and its derivatives shall be construed accordingly.

1.9 "**Model Clauses**" means the Standard Contractual Clauses for the transfer of personal data (Decision 2021/914/EU), as they may be amended or replaced from time to time, in respect of transfers from the European Economic Areas ("**EEA**") to countries outside the EEA (including the United Kingdom ("**UK**")) and means the Standard Contractual Clauses for the transfer of personal data to Processors (Decision 2010/87/EU, or "**UK Clauses**") in respect of transfers from the UK to countries which are not subject to an adequacy decision under the UK GDPR.

1.10 "**Personal Data**" means any information or data that alone or together with any other information relates to an identified or identifiable natural person ("**data subject**"), or as otherwise defined as "personal data" or "personal information" under Privacy Laws. 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.

1.11 "**Privacy Laws**" means any law, statute, directive, or regulation, including any and all legislative and/or regulatory amendments or successors thereto, regarding privacy, data protection, information security obligations and/or the processing of Personal Data (including where applicable, the GDPR, UK GDPR, the California Consumer Privacy Act ("**CCPA**") and similar US state and federal laws) to which a party to this DPA is subject and which are applicable to the Solutions provided.

1.12 "**Provider**" means the party from which Dell is purchasing Solutions under the Provider Agreement and its Representatives.

1.13 "**Provider Agreement**" means the agreement or agreements between Dell and Provider pursuant to which Dell is purchasing Solutions from Provider, including a Master Relationship Agreement.

1.14 "**Processing**", "**processed**" or "**process**" means any operation or set of operations performed upon Dell Data whether or not by automated means, including access, receipt, collection, recording, organization, structuring, adaptation, alteration, retrieval, consultation, retention, storage, transfer, disclosure (including disclosure by transmission), dissemination or otherwise making available, restriction, alignment, combination, use, blocking, erasure and destruction.

1.15 "**Processor**" means an entity which processes the Personal Data on behalf of the Controller in order to perform Solutions purchased by Dell under the Provider Agreement, or as otherwise defined as "Service Provider" under the Privacy Laws.

1.16 "**Representatives"** means any employee, officer, agent, consultant, auditor, Subcontractor, outsourcer or other third party acting on behalf of Provider or under the apparent authority of Provider in connection with providing Solutions.

1.17 **"Sell**" or "**sale**" or means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or any other non-monetary valuable consideration. Sale does not include Personal Data shared or transferred by Dell to Provider for the provision of Solutions on behalf of Dell under the Agreement.

1.18 "**Subcontractors**" means any third party, including all subcontractors, acting for or on behalf of Provider, providing Solutions

to Dell, or to whom Provider has assigned or delegated its contractual obligations to Dell. "Subcontractors" does not include employees of Provider.

1.19 "**Solutions**" means any hardware, software (including third party components), software-as-a-service, services, or hosting services provided to Dell or a Dell customer pursuant to the Provider Agreement.

1.20 "**UK GDPR**" means the GDPR as retained under United Kingdom domestic law further to the exit of the UK from the European Union, to be read alongside the UK Data Protection Act 2018, as may be amended from time to time.

1.21 "**User Tracking Data**" means data associated with online or mobile users that records user information, interactions or behavior, user clicks or reaction to or interaction with content, advertising or any other activity, or in connection with tracking activities related to behavioral advertising.

2. **CONFIDENTIAL INFORMATION.** All Dell Data is "Confidential Information" as defined in (a) the NDA; or (b) if Provider and Dell have not entered into an NDA, the Provider Agreement. Any exclusions to the definition of "Confidential Information" in the NDA or the Provider Agreement shall not apply to the definition of Dell Data. Provider shall treat Dell Data as Confidential Information for as long as such Dell Data is in Provider's possession or control, including when the Dell Data is held in archive, back up or business continuity/disaster recovery systems and shall ensure that all Representatives are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3. **PROVIDER OBLIGATIONS**

3.1 Role of Parties. The parties agree that Dell is the Controller of Personal Data and Provider is the Processor of such data, except where Dell acts as a Processor of Personal Data, in which case Provider is a Subprocessor.

3.2 Processing. Provider shall (and shall ensure that its Representatives shall) only process Dell Data in accordance with Dell's documented instructions, including with regard to international transfers of Dell Data. Provider shall immediately inform Dell in writing if, in its opinion, an instruction from Dell infringes applicable Privacy Laws. Provider shall not knowingly process any Dell Data in a way that results in Dell being in breach of its obligations under Privacy Laws. Dell hereby instructs and authorizes Provider to process Dell Data for the sole and exclusive purpose of performing Provider's obligations to Dell under and in accordance with (a) the Provider Agreement; (b) Dell's and its agents' written instructions; (c) Privacy Laws; and (d) this DPA (collectively, the "Applicable Agreements"). Where Provider tracks users' online or mobile activities, the obligations and requirements set out in this DPA in relation to Personal Data extend to User Tracking Data.

3.3 Personal Data Processing. Provider shall process Personal Data as part of the provision of the Solutions as described below. Dell may make reasonable amendments to this section by written notice to Provider from time to time as Dell reasonably considers necessary;

(a) Subject Matter, Purpose and Duration. Provider shall process the Personal Data (for the term of the Provider Agreement as extended or amended) for the purpose of providing the Solutions specified in the Provider Agreement.

(b) Data Subjects. Personal Data processing may relate to any of the following data subjects: past, present and prospective employees, customers, end users, web site visitors, partners, clients, advisors, consultants, suppliers, contractors, subcontractors and agents, beneficiaries and relatives.

(c) Types of Personal Data. Personal Data processing may involve any of the following: Personal Data (including special categories of data if appropriate): (i) contact details (e.g. name, address, e-mail address, contact details, local time zone information); (ii) employment details (e.g. company name, job title, grade, demographic and location data), (iii) IT systems information (which may include user ID and password, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies), (iv) data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails), (v) details of goods or services provided to or for the benefit of data subjects, and (vi) financial details (e.g. credit, payment and bank details).

3.4 Prohibition and Limitations on Disclosure and Use. Provider shall not process, sell, transfer or otherwise disclose Dell Data to, or permit processing by its Representatives or any Third Party except (a) on a need-to-know-basis related to the provision of the Solutions where instructed by Dell; (b) to the extent necessary to provide the Solutions; (c) as permitted under the Applicable Agreements; or (d) if required by Applicable Law. If provider is required by Applicable Law to transfer, disclose or permit processing of Dell Data by a third party, Provider will promptly notify Dell in advance of such requirement and cooperate with Dell to limit the extent and scope of such transfer, disclosure or processing. Provider represents and warrants, i.e. certifies, that it understands the prohibitions and limitations regarding its use and all other processing activities and related purposes as outlined in this Agreement regarding Dell Data, particularly in this Section 3.4, and will comply with them.

3.5 Compliance with Privacy Laws. Provider agrees to comply with any and all Privacy Laws applicable to the provision of the Solutions and its processing of Personal Data.

3.6 Return and Destruction. Upon termination of the Provider Agreement or upon written request from Dell, whichever comes first, Provider shall, and shall ensure that its Representatives and Subcontractors shall, immediately cease all processing of Dell Data and return any Dell Data to Dell (by secure file transfer in such format as reasonably notified by Dell to Provider) or, at the direction of Dell, dispose of, destroy, or render permanently anonymous all Dell Data, in each case using the security measures set out herein and certifying in writing to Dell once the disposition, destruction or anonymisation has been fully completed. If Applicable Law does not permit Provider to destroy the Dell Data, Provider shall not use the Dell Data for any purpose other than as required by such Applicable Law and shall remain bound at all times with the provisions of the Applicable Agreements for as long as the Dell Data is in Provider's possession or control.

3.7 Notifications and Assistance. Taking into account the nature of the processing, Provider shall (and shall ensure its Subcontractors shall) assist Dell by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Dell's obligations (as reasonably understood by Dell) to respond to requests to exercise data subject rights

under Privacy Laws in respect of the Personal Data. If Provider is contacted by a person with a request, inquiry or complaint regarding their Personal Data in connection with the Solutions, Provider shall (a) promptly and in any event within two calendar days provide Dell with written notice of such request, inquiry or complaint; and (b) provide to Dell all reasonable cooperation, assistance, information and access to Personal Data in its possession, custody or control as is necessary for Dell to respond to such request, inquiry or complaint promptly and within any timeframe required by Privacy Laws. Provider shall not respond to such request, inquiry or complaint unless so instructed in writing by Dell.

3.8 Privacy Impact Assessments. Provider shall provide cooperation and assistance to Dell in connection with any privacy impact assessment(s) which Dell may carry out in relation to the processing of Personal Data undertaken by the Provider, including any prior consultation(s) with supervisory authorities or other competent data privacy authorities which Dell reasonably considers to be required by applicable Privacy Laws.

3.9 Controller status. Provider shall not determine the purposes and means of the processing of the Personal Data without Dell's prior explicit agreement in writing, in which case Provider shall be deemed a controller and shall only process the Personal Data as agreed in writing with Dell and in full compliance with all applicable Privacy Laws.

4. **INTERNATIONAL TRANSFERS.**

4.1. Transfers out of the EEA. Provider may only transfer Personal Data from EEA countries or the UK to countries outside the EEA or the UK with the prior written consent of Dell, provided that such transfer is strictly necessary for the provision of the Solutions, is subject to the terms set out in the Model Clauses and Provider complies with all obligations imposed on a "data importer" for Controller to Processor transfers, and imposed on a data exporter for Processor to Controller transfers as set out in such Clauses. Where the Model Clauses apply to a transfer in accordance with this clause, they shall be incorporated into and form part of the DPA by reference. Dell may, by at least 30 (thirty) calendar days' written notice to Provider, from time to time make any variations to the Model Clauses which Dell considers to be reasonably required as a result of any change in, or decision of, a competent authority under Privacy Laws so as to allow transfers to be made or continue to be made in compliance with Privacy Laws. If Dell gives notice to vary the Model Clauses, Provider shall promptly co-operate (and ensure that any affected Subcontractors promptly co-operate) to ensure the variations required by Dell are implemented. If the Model Clauses cease to provide a valid legal basis for the transfer of personal data to countries outside the EEA or the UK, the parties shall without undue delay meet to agree in good faith what alternative methods are available to facilitate the transfer of the Personal Data in accordance with applicable Privacy Law and implement an agreed alternative method as soon as practicable. This may include the parties agreeing to enter into an alternative data transfer method where available and appropriate.

4.2. Transfers out of Asia Pacific. For countries located within the Asia Pacific region, Provider shall obtain Dell's prior written consent where Personal Data will be transmitted by the Provider outside the country from which it was originally collected unless otherwise required by the Applicable Agreements.

4.3. Transfers out of countries with data export requirements. If any Privacy Laws require that further steps be taken in relation to any applicable data export restrictions to permit the transfer of Personal Data under the Agreement to Provider (including its Subcontractors), Provider will comply with such data protection requirements including executing any applicable data transfer agreements (e.g. standard contractual clauses) or an alternative solution to ensure that appropriate safeguards are in place for such transfer.

5. **APPROPRIATE SECURITY SAFEGUARDS.** Provider shall process the Dell Data in a manner that ensures appropriate security of the Dell Data (including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage) using appropriate technical and/or organisational measures which ensure a level of security commensurate to the risk, including as appropriate: (a) the encryption of the Dell Data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (c) the ability to restore the availability and access to the Dell Data in a timely manner in the event of a physical or technical incident, and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Dell Data. In assessing the appropriate level of security, Provider shall take account in particular of the risks that may be presented by the processing of the Dell Data, in particular from a Data Breach. Provider agrees to have in place and maintain as a minimum those information security measures set out in this DPA. As part of its compliance with this clause, Provider shall have and maintain appropriate and industry-standard physical, organizational and technical processes, security standards, guidelines, controls and procedures ("**Policies**") to protect against any Data Breach ("**Appropriate Safeguards**"). Provider shall regularly, but in no event less than annually, evaluate, test and monitor the effectiveness of its Appropriate Safeguards and shall promptly adjust and update Appropriate Safeguards as reasonably warranted by such results. Provider shall, upon request, provide Dell with a written description of the Appropriate Safeguards. Provider shall provide Dell with access to relevant documentation and reporting on the implementation, certification, effectiveness and remediation of the Appropriate Safeguards. Provider represents, warrants and covenants that Provider and its Subcontractors do and shall implement and maintain Policies which:

5.1 Risk Management. Evaluate organizational and administrative risks no less than annually, and system and technical risks no less than quarterly.

5.2 Asset Management. (a) Identify all equipment and media used in the processing of Dell Data; (b) assign responsibility for all equipment and media to one or more custodians; and (c) require regular reviews of the asset inventory for accuracy and to identify missing equipment and media.

5.3 Access Control and Identity Management Policies. Prior to access to Dell Data, (a) all data and system access rights are assigned to individuals according to their documented responsibilities and the principle of least privilege; (b) all user and administrator accounts are assigned to individuals and required to have strong passwords, password rotation, failed authentication locks and session timeouts; and (c) issuance of privileged access accounts require management approval and are held to strict security standards.

5.4 Awareness and Training Policies. Address (a) information security threats and best practices; (b) information security policies,

procedures, and controls in place to protect Dell Data; and (c) each Representative's roles and responsibilities in the protection of Dell Data.

5.5 Accountability Policies. Ensure that (a) all account actions can be traced to the individual using the account, (b) the time, date and type of action is recorded for all privileged account actions and all account actions affecting Dell Data, (c) all recorded account actions are actively monitored and can be easily retrieved for analysis, and (d) consequences for policy violations are established, communicated and acted upon.

5.6 Contingency Planning Policies. Define roles and responsibilities and provide clear guidance and training on the proper handling of contingency events including (a) natural threat events such as floods, tornadoes, earthquakes, hurricanes and ice storms; (ii) accidental threat events such as chemical spills and mechanical or electrical failures; and (iii) intentional acts such as privacy and security breaches, bomb threats, assaults and theft.

5.7 System Maintenance Policies. Are related to (a) structured vulnerability management, including regular scanning, penetration testing, risk analysis and timely patching; (b) change management, including documentation of the purpose, security impact analysis, testing plan and results, and authorization for all changes; (c) configuration management, including secure baseline configurations; and (d) monitoring to detect and generate alerts for unauthorized changes.

5.8 System and Communications Protection Policies. Preserve the confidentiality, integrity and availability of Dell Data, including (a) physical controls that restrict and monitor access to systems that process Dell Data; (b) technical and administrative controls that protect against malicious software and malicious actors; (c) strong encryption of data in transit across untrusted and public networks and, in the case of Highly Restricted Data, at rest in all locations where it is stored; (d) periodic encryption key rotation and management; (e) prohibition of Highly Restricted Data and Personal Data being processed in non-production environments; (f) regular security control reviews and effectiveness testing; and (vii) strong technical and administrative controls regarding remote access and mobile devices.

5.9 Media Protection Policies. Ensure that media containing Dell Data is securely handled, including (a) strong encryption of Dell Data on all mobile devices and removable storage; (b) requirement for secure sanitization and destruction methods for media that at any time held Dell Data; and (c) requirement that all media, including paper, containing unencrypted Dell Data be stored in a secure location.

6. **PAYMENT CARD INFORMATION.** Prior to processing any cardholder data in connection with a Provider Agreement, Provider must comply, and remain in compliance, at their own expense, with the Payment Card Industry Data Security Standard ("**PCI DSS**"). Prior to processing any cardholder data and annually thereafter, Provider must submit an attestation to Dell stating that they are current in their PCI Report on Compliance/Self Assessment Questionnaire and PCI Quarterly Network Scan filings and that they remain PCI-compliant, as well as any documentation supporting such attestation as reasonably requested by Dell. If at any point Provider is not in compliance with the PCI DSS or is unable or unwilling to produce adequate evidence of compliance, Provider shall be in breach of the Provider Agreement and Dell may immediately terminate the Provider Agreement without liability to Dell.

7. **INFRASTRUCTURE SECURITY & CONNECTIVITY.** If (a) the Solutions include application, website, data or system hosting; (b) network connectivity is required to provide the Solutions; or (c) the Solutions are dependent on the integrity of Provider's environment, the following requirements shall apply:

7.1 Network Access. The connection and mechanism to transmit Dell Data between Provider and Dell shall be through a Dell I/T-approved secure solution. Duration of access shall be restricted to only when access is required. Provider shall use Appropriate Safeguards to protect against any compromise, unauthorized access or other damage to Dell's network and to secure the Provider's networks and I/T environments associated with the Solutions. Upon request, Provider shall provide Dell with a high level network diagram that outlines Provider's I/T network supporting the Solutions.

7.2 Audit. Upon request, Provider shall provide a controls audit report and remediation effort, such as a SSAE 16 or information security audit performed within the past year, as applicable to the Solutions. The audit shall include an assessment of Provider's applicable general controls and security processes and procedures to ensure compliance with Privacy Laws and industry standards. The audit shall be at Provider's expense as part of Provider's ongoing information security program to evaluate Provider's general security controls.

7.3 Testing. In addition to Provider's internal control programs, Provider will have independent penetration tests performed on its environment as relevant to this DPA not less than once year, and will perform security vulnerability scans not less frequently than quarterly. Provider commits to remediate all vulnerabilities identified in a timeframe commensurate with the risk, or as agreed upon with Dell.

8. **SOLUTION SECURITY**

8.1 Vulnerabilities. Provider shall have controls in place to identify any security vulnerabilities in the Solutions during development and after release. Provider shall provide Dell written notice of (a) publicly-acknowledged vulnerabilities/zero day exploits within five business days of the public acknowledgement; and (b) internally-known yet publicly-undisclosed vulnerabilities/zero day exploits within ten business days of their discovery. Provider commits to remediate all vulnerabilities identified in the Solutions at Provider's expense, and to remediate vulnerabilities with a base score above 4 as defined by Common Vulnerability Scoring System in a timeframe commensurate with the risk or as agreed upon with Dell. Provider's use of open source code shall not alter Provider's responsibility to identify and remediate vulnerabilities as described here.

8.2 Coding Practices. Provider agrees (a) to use industry secure-coding practices (for example, Microsoft's Software Development Lifecycle, Cigital Software Security Touchpoints, OWASP standards or Sans Top 25); (b) the Solutions are designed based on industry secure-coding practices; and (c) information security is addressed throughout the development life-cycle. The Solutions' processes, direct capabilities, and other necessary actions shall comply with all PCI standards and Privacy Laws.

8.3 Security Assessments. Provider shall submit the results and remediation efforts of an independent security assessment for all Solutions that (a) are customer facing, including websites, shipped with or installed on customer systems; or (b) process Highly

Restricted Data. The assessment scope and remediation efforts must be agreed upon by Dell and addressed to Dell's satisfaction prior to acceptance of such Solutions.

9. **DATA BREACH.** Provider shall notify Dell not later than 24 hours after becoming aware of an actual or reasonably suspected Data Breach. Such notification must be provided, at a minimum, by email with a read receipt to privacy@dell.com and with a copy to Provider's primary business contact within Dell. In facilitating investigation and remediation of a Data Breach, Provider shall cooperate fully with Dell. Provider shall not inform any third party of any Data Breach without first obtaining Dell's written consent except as may be strictly required by Privacy Laws in which case Provider will, unless prohibited by law, notify Dell in advance of informing any such third party and cooperate with Dell to limit the scope of the information disclosed to what is required by Privacy Laws. Details of any complaint received by Provider related to processing of Highly Restricted, Personal Data or User Tracking Data shall be promptly sent to Provider's Dell business contact. Provider shall reimburse Dell for costs Dell incurs in responding to, remediating, and/or mitigating damages caused by a Data Breach or in following up a complaint by an individual data subject or a regulator. Provider shall take all necessary and appropriate corrective actions, including as may be instructed by Dell or Privacy Laws, to remedy or mitigate any Data Breach. Provider shall, to the extent such information is known or available to Provider at the time, notify Dell of the following: (a) the nature of the Data Breach including, where possible, the categories and approximate number of data subjects affected and number of Personal Data records concerned; (b) the name and contact details of Provider's data protection officer or other contact point where more information can be obtained; (c) a description of the likely consequences of the Data Breach; and (d) a description of the measures taken or proposed to be taken by Provider to address the Data Breach, including (where appropriate) measures to mitigate its possible adverse effects. Where it is not possible for Provider to provide the above information at the same time, Provider shall provide the information in phases without undue further delay. The information must be provided, at a minimum, by email with a read receipt to privacy@dell.com and with a copy to Provider's primary Dell business contact.

10. **REPRESENTATIVES AND SUBCONTRACTORS**

10.1 Restrictions. Unless expressly permitted by the Provider Agreement Provider shall not (a) transfer; (b) sell or disclose; (c) subcontract the processing of; or (d) permit the processing of, Dell Data by or to any Subcontractors without the prior written authorisation of Dell.

10.2 Requirements for Subcontractors and Representatives. Provider shall take all reasonable steps to ensure the reliability of Representatives and Subcontractors that may have access to the Dell Data, including carrying out appropriate background checks (where permitted by Applicable Law) and carrying out adequate due diligence to ensure that any Representatives and Subcontractors are capable of providing the level of protection for Dell Data required by this DPA. Provider shall ensure Representatives and Subcontractors are appropriately trained in the handling and secure processing of Dell Data under Privacy Laws. If Provider is permitted by Dell to transfer Dell Data to a Subcontractor, Subcontractor shall comply with Section 4 "International Transfers" of this DPA as if Provider were Dell and the Subcontractor was the Provider.

10.3 Subcontractor Agreement. Agreements by and between Provider and the Representatives and Subcontractors authorized to Process Dell Data ("Subcontractor Contracts") shall include substantially equivalent restrictions and conditions as this DPA and shall be in writing. Provider shall have sole liability for all acts or omissions of Representatives and Subcontractors. Provider shall provide Dell with a copy of Subcontractor Contracts upon request.

10.4 Subcontractor Audits. Provider shall audit each of its Subcontractors that process Dell Data at least once every twelve months and more frequently in the event of a Data Breach. If the audit reveals any compliance deficiencies, breaches and/or failures by the Subcontractor, Provider shall promptly notify Dell and use all reasonable efforts to work with the Subcontractor to remedy the same promptly. If, within Dell's reasonable discretion, a satisfactory remedy cannot be implemented within a reasonable time, Dell may instruct Provider not to continue using the Subcontractor to provide Solutions to Dell, in which case Provider shall be required, as instructed by Dell, to promptly return or delete any Dell Data in the Subcontractor's possession or control. To the extent not restricted by confidentiality, Provider shall share the results of such audits with Dell upon prior written request. Dell agrees that it will comply with the confidentiality obligations in this DPA in relation to any disclosed audit results.

11. **CALL RECORDINGS**. If Provider processes call recordings, Provider shall establish strong controls for processing call recordings containing Highly Restricted data or Personal Data. Access to and processing of call recordings shall be limited only to Representatives necessary to provide the Solutions and in compliance with Applicable Law. Provider shall keep a recorded log of all access made to call recordings. Provider shall delete all call recordings containing Personal Data as soon as reasonably possible after the recordings have served their purpose and within such time frames as are set down by Privacy Laws and applicable security standards, but in any event, no later than 90 days (21 days in EMEA), unless otherwise approved in writing by Dell's Privacy Office. Provider shall record only a small sample of the call volume and within such time frames required by Privacy Laws. For recordings containing payment card or other Highly Restricted data, Provider shall store the call recordings in voice stream format (and not as data files), unless all payment card data is removed from the recordings or rendered unreadable/inaudible at the time of recording.

12. **CANADIAN DATA**. If Provider processes Personal Data concerning persons located in Canada in the course of providing Solutions, Provider and Dell agree to the additional obligations and requirements in this Section 12. Provider shall not take any actions or make any omissions that will cause Dell to be in contravention of the Personal Information Protection and Electronic Documents Act (Canada), as amended or supplemented from time to time, and any other Canadian federal or provincial legislation governing the processing of Personal Data. Provider shall keep all data, databases or other records containing Personal Data processed in connection with the Solutions logically isolated and separate from any information, data, databases or other records processed by Provider for itself or for third parties. Provider shall designate and identify to Dell an individual responsible for the oversight of the Personal Data. Dell may be required to disclose, without advance notice or consent, Confidential Information of Provider to authorities in connection with any investigation, audit or inquiry in connection with the Solutions. Provider shall not move, remove or transmit any Personal Data from Provider's facilities without the express consent of Dell and without Provider shall not move, remove or transmit any Personal Data from Provider's facilities without the express consent of Dell and without using appropriately secure technology to protect such information while in transit. If Provider is contacted by a person with a request, inquiry or complaint regarding their Personal Data in connection with the Solutions, Provider shall promptly refer such person to Dell.

13. **SUPPLEMENTAL AGREEMENTS TO THE DPA.**

13.1 EU Standard Contractual Clauses. If Provider processes Personal Data that is subject to the GDPR, in the course of providing Solutions, Provider and Dell hereby agree to, and Provider shall comply with, the EU Standard Contractual Clauses – Controller to Processor, the EU Standard Contractual Clauses – Processor to Controller, and all annexes attached thereto. Should the EU Commission issue and require use of amended or updated EU Standard Contractual Clauses, such clauses shall be incorporated herein by this reference automatically and supersede prior Standard Contractual Clause versions as of the date they become effective as set by the EU Commission.

13.2 UK Standard Contractual Clauses. If provider processes Personal Data subject to the UK GDPR in the course of providing Solutions, Provider and Dell hereby agree to, and Provider shall comply with, the UK Standard Contractual Clauses ("**UK Clauses**"), including Appendices 1 and 2 attached hereto. Should the appropriate United Kingdom regulatory authority issue and require use of amended or updated UK standard contractual clauses, such clauses shall be incorporated herein by this reference automatically and supersede prior clause versions as of the date they become effective under United Kingdom law.

13.3 HIPAA Compliance. If Provider accesses, retains, is exposed to, or becomes aware of "Protected Health Information" as defined in 45 C.F.R. § 164.501 of participants of Dell Inc. Comprehensive Welfare Benefits Plan in the course of providing Solutions, Provider and Dell hereby agree to and Provider shall comply with the HIPAA US Subcontractor Agreement and the HIPAA Business Associate Agreement.

13.4 Authority. **PROVIDER REPRESENTS AND COVENANTS TO DELL THAT PROVIDER, INCLUDING ANY REPRESENTATIVE OF PROVIDER ACCEPTING THIS DPA ON ITS BEHALF, IS AUTHORIZED TO BIND PROVIDER TO THE EU STANDARD CONTRACTUAL CLAUSES INCLUDING APPENDIX 1 AND APPENDIX 2 THERETO, THE HIPAA SUBCONTRACTOR AGREEMENT AND THE BUSINESS ASSOCIATE AGREEMENT.**

14. **DELL SUBSIDIARY RIGHTS**. Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA. Where the Solutions include the processing by Provider Representatives of Dell Data on behalf of Dell direct and indirect subsidiaries, each such Dell direct and indirect subsidiary is intended to be a third party beneficiary and may enforce the terms of this DPA as a third party beneficiary against Provider in respect of that Dell subsidiary's own Dell Data, as if such Dell subsidiary were a party to this DPA and/or any Provider Agreements.

15. **AUDITS**. Provider shall make available to Dell upon request all information necessary to demonstrate compliance with its obligations under this DPA and shall permit Dell or its designee to (a) audit Provider's compliance with this DPA; and (b) inspect any Personal Data in the custody or possession of Provider. Provider shall promptly respond to all inquiries from Dell with respect to Provider's handling of Personal Data.

16. **RECORD KEEPING**. Provider shall maintain a written or electronic record of processing activities carried out on behalf of Dell containing the following minimum information: (a) name and contact details of Provider and its Subcontractors, (b) name and contact details of its data protection officer (if any), (c) the categories of processing carried out on behalf of each controller, (d) any transfers of personal data to countries outside the EEA and documentation showing Model Clauses are in place, (e) a general description of the technical and organisational security measures in place to safeguard the Personal Data including the measures in this DPA.

17. **INDEMNIFICATION.** Provider shall defend, indemnify and hold harmless Dell and Dell's directors, officers, employees, representatives, and agents from and against any and all claims, actions, demands, and legal proceedings and all liabilities, damages, losses, judgments, authorized settlements, costs, fines, penalties and expenses including reasonable attorneys' fees arising out of or in connection with (a) Provider's breach of this DPA; (b) Provider's failure to comply with the PCI DSS; or (c) violation by the Provider of any Privacy Laws.

18. **MISCELLANEOUS.**

18.1 Survival. Provider's obligations under this DPA shall survive the termination or expiration of the DPA, NDA, and the Provider Agreement and continue in effect for as long as Provider continues to process Dell Data.

18.2 Notices. Legal notices shall be made in writing to the Notice Address set forth in the Provider Agreement. Written notice made by facsimile, overnight courier, registered mail or certified mail and sent to the Dell Notice Address or Provider Notice Address (or to successor individuals and addresses that have been properly noticed to the other party) are deemed to be effective upon sending. All other written communications, deliveries or business notices between Provider and Dell required by, permitted by or pertaining to this DPA shall be effective when received.

18.3 Assignment. Provider may not assign or transfer this DPA, in whole or in part, whether voluntarily, by contract or by merger (whether that party is the surviving or disappearing entity), stock or asset sale, consolidation, dissolution, through government action or order, or otherwise without the prior written consent of Dell. Any attempt to assign or transfer this DPA other than in accordance with this Section will be null and void. Dell may assign the DPA without Provider consent.

18.4 Waiver/Amendment. No waiver of any term or condition is valid unless in writing and signed by authorized representatives of both parties, and shall be limited to the specific situation for which it is given. No amendment or modification to this DPA shall be valid unless set forth in writing specifically referencing this DPA and signed by authorized representatives of both parties. No other action or failure to act shall constitute a waiver of any rights.

18.5 Entire agreement. This DPA sets forth the entire agreement and understanding of the parties relating to the subject matter herein, and replaces all prior or contemporaneous discussions and agreements between the parties, both oral and written.

18.6 Independent contractor. In performing Provider's responsibilities pursuant to this DPA, it is understood and agreed that Provider is at all times acting as an independent contractor and that Provider is not a partner, joint venturer, or employee of Dell. It is expressly agreed that Provider will not for any purpose be deemed to be an agent, ostensible or apparent agent, or servant of Dell, and the parties agree to take any and all such action as may be reasonably requested by Dell to inform the public and others utilizing the professional services of Provider of such fact.

18.7 Additional agreements. Each of the parties hereto agrees to execute any document or documents that may be requested from

time to time by the other party to implement or complete such party's obligations pursuant to this DPA, Privacy Law or Applicable Law. The parties agree to take such reasonable actions as are necessary to amend this DPA from time to time as is necessary for Dell to comply with Privacy Law and Applicable Law.

18.8 Interpretation. Any ambiguity in this DPA will be resolved in favor of a meaning that permits Dell to comply with Privacy Law and Applicable Law.

18.9 Governing Law; Venue. The DPA and any disputes between Provider and Dell (and their Representatives) including without limitation, tort and statutory claims arising under or relating in any way to the DPA or any relationships contemplated herein shall be governed and construed in accordance with the laws of the State of Texas, U.S., exclusive of any provisions of the United Nations Convention on the International Sale of Goods and without regard to its principles of conflicts of law. Provider and Dell irrevocably submit and consent to the exclusive jurisdiction and venue of the U.S. District Court for the Western District of Texas (Austin Division) or if there is no basis for Federal jurisdiction, then any claims must be brought in the Texas State District Court in Williamson County, Texas. The parties agree that such courts shall be the exclusive proper forum for the determination of any claim or dispute arising out of, or in connection with, the DPA and waive any objection to venue or convenience of forum.

EU STANDARD CONTRACTUAL CLAUSES - CONTROLLER TO PROCESSOR

For the purpose of EU Standard Contractual Clauses – Controller to Processor, the name of data exporting organization is Dell Products, an unlimited company organized under the laws of Ireland with registered number 191034 and whose registered office is at 70 Sir John Rogerson's Quay, Dublin 2, Ireland together with all other Dell group entities (as defined below), each such Dell entity having the right to enforce the terms of these Standard Contractual Clauses as a third party beneficiary against the data importer in respect of any personal data which are processed by such Dell entity as a controller, as if such Dell entity were entering into its own separate set of Standard Contractual Clauses with the data importer.

Dell group entity means a party or any business entity at any time controlling, controlled by or under common control with Dell Products. "**Control**" means in respect of a company, the power of a person to directly or indirectly secure that the affairs of the company are conducted in accordance with the wishes or directions of that person. "Controlling", "controlled by" and "under common control" shall be construed accordingly.

SECTION I

CLAUSE 1: **PURPOSE AND SCOPE**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

CLAUSE 2: **EFFECT AND INVARIABILITY OF THE CLAUSES**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

CLAUSE 3: **THIRD-PARTY BENEFICIARIES**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

CLAUSE 4: **INTERPRETATION**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

CLAUSE 5: **HIERARCHY** In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

CLAUSE 6: **DESCRIPTION OF THE TRANSFER(S)** The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

CLAUSE 7 **– DOCKING CLAUSE [Intentionally omitted.]**

SECTION II – OBLIGATIONS OF THE PARTIES

CLAUSE 8: **DATA PROTECTION SAFEGUARDS** The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

CLAUSE 9: **USE OF SUB-PROCESSORS**

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

CLAUSE 10: **DATA SUBJECT RIGHTS**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

CLAUSE 11: **REDRESS**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    (ii) refer the dispute to the competent courts within the meaning of Clause 18.
(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

CLAUSE 12: LIABILITY

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

CLAUSE 13: SUPERVISION

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 14: LOCAL LAWS AND PRACTICES AFFECTING COMPLIANCE WITH THE CLAUSES

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
    (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
    (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
    (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 15: OBLIGATIONS OF THE DATA IMPORTER IN CASE OF ACCESS BY PUBLIC AUTHORITIES

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
    (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
    (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

***CLAUSE 16:* NON-COMPLIANCE WITH THE CLAUSES AND TERMINATION**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

***CLAUSE 17:* GOVERNING LAW**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Luxembourg.

***CLAUSE 18:* CHOICE OF FORUM AND JURISDICTION**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

DATA EXPORTER. The data exporter is identified at the start of the Clauses and is a provider of IT products and services. The data exporter is the Controller and has appointed the data importer to provide certain products and/or services as specified in the Provider Agreement as its Processor. To facilitate the provision of these products and services, the data exporter may provide to the data importer access to the personal data described below.

DATA IMPORTER. The data importer is a signatory to the Clauses and a provider of products and/or services. The data importer will be the recipient of personal data which is exported by the data exporter to the data importer as described below.

B. DESCRIPTION OF TRANSFER

DATA SUBJECTS. The personal data transferred may concern the following categories of data subjects:

- Past, present and prospective employees and partners;
- Past, present and prospective clients, customers, end users, web site visitors;
- Past, present and prospective advisors, consultants, suppliers, contractors, subcontractors and agents;
- Beneficiaries and relatives.

CATEGORIES OF DATA. The data subjects' personal data transferred may concern the following categories of data:

1. Contact details (which may include name, address, e-mail address, phone and fax contact details and associated local time zone information);
2. Employment details (which may include company name, job title, grade, demographic and location data);
3. IT systems information (which may include user ID and password, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies);
4. Data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails);
5. Details of goods or services provided to or for the benefit of data subjects;
6. Financial details (e.g. credit, payment and bank details).

SPECIAL CATEGORIES OF DATA (IF APPROPRIATE). Personal data transferred may include information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union opinions, memberships or activities, social security files, and data concerning health (including physical or mental health or condition), sexual life and information regarding criminal offences or alleged offences and any related court proceedings and shall include special categories of data as defined in Article 8 of the Directive 95/46/EC.

PROCESSING OPERATIONS. The personal data transferred may be subject to the following processing activities: Any operation with regard to personal data irrespective of the means applied and procedures, in particular the obtaining, collecting, recording, organizing, storage, holding, use, amendment, adaptation, alteration, disclosure, dissemination or otherwise making available, aligning, combining, retrieval, consultation, archiving, transmission, blocking, erasing, or destruction of data, the operation and maintenance of systems, management and management reporting, financial reporting, risk management, compliance, legal and audit functions and shall include "processing" which shall have the meaning given to such term in the Directive.

TRANSFER DETAILS. The frequency of the transfer (e.g., whether the data will be transferred on a one-off or continuous basis), purpose of the data transfer and further processing, period for which the personal data will be retained or the criteria used to determine that period and details concerning any transfers to sub-processors will be as set forth in the corresponding product or services agreement to which these standard contractual clauses relate.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 is the:

DATA PROTECTION COMMISSION OF IRELAND
21 FITZWILLIAM SQUARE SOUTH
DUBLIN 2
D02 RD28
IRELAND

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

SECURITY PRACTICES. Data importer has implemented corporate information security practices and standards that are designed to safeguard data importer's corporate environment and to address business objectives across the following areas: (1) information security, (2) system and asset management, (3) development, and (4) governance. These practices and standards are approved by the data importer's executive management and are periodically reviewed and updated where necessary. Data importer shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data and sensitive personal data throughout its lifecycle. Key policies should be reviewed at least annually.

ORGANIZATIONAL SECURITY. It is the responsibility of the individuals across the data importer's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, data importer's Information Security ("**IS**") function is responsible for the following activities:

1. **Security strategy** – the IS function drives data importer's security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS function also carries out risk assessments and risk management activities, and manages contract security requirements.
2. **Security engineering** – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.
3. **Security operations** – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.
4. **Forensic investigations** – the IS function works with Security Operations, Legal, Global Privacy Office and Human Resources to carry out investigations, including eDiscovery and eForensics.
5. **Security consulting and testing** – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

ASSET CLASSIFICATION AND CONTROL. Data importer's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that data importer might track include:

- information assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information
- software assets, such as identified applications and system software
- physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

EMPLOYEE SCREENING, TRAINING AND SECURITY

1. **Screening/background checks:** Where reasonably practicable and appropriate, as part of the employment/recruitment process, data importer shall perform screening/background checks on employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to data importer's networks, systems or facilities.
2. **Identification:** Data importer shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other data importer entities or customers for whom the employee is providing services.
3. **Training:** Data importer's annual compliance training program includes a requirement for employees to complete a data protection and information security awareness course and pass an assessment at the end of the course. The security awareness course may also provide materials specific to certain job functions.
4. **Confidentiality:** Data importer shall ensure its employees are legally bound to protect and maintain the confidentiality of any personal data they handle pursuant to standard agreements.

PHYSICAL ACCESS CONTROLS AND ENVIRONMENTAL SECURITY

1. **Physical Security Program:** Data importer shall use a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably practicable. Data importer's security team works closely with each site to determine appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which personal data is processed and continually monitor any changes to the physical infrastructure, business and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniqueness in business practice and expectations of data importer. Data importer balances its approach towards security by considering elements of control that include architecture, operations and systems.
2. **Physical Access controls:** Physical access controls/security measures at data importer's facilities/premises are designed to meet the following requirements:

(a) access to data importer's buildings, facilities and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to the data importer. Only personnel associated with data importer are provided access to data importer's facilities and physical resources in a manner consistent with their role and responsibilities in the organization;

(b) relevant data importer facilities are secured by an access control system. Access to such facilities is granted with an activated card only;

(c) all persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g. a badge or keycard assigned to one individual) by the IS function. Individuals issued with unique physical access credentials are instructed not to allow or enable other individuals to access the data importer's facilities or resources using their unique credentials (e.g. no "tailgating"). Temporary (up to 14 days) credentials may be issued to individuals who do not have active identities where this is necessary (i) for access to a specific facility and (ii) for valid business needs. Unique credentials are non-transferable and if an individual cannot produce their credentials upon request they may be denied entry to data importer's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative;

(d) employees are regularly trained and reminded to always carry their credentials, store their laptops, portable devices and documents in a secure location (especially while traveling) and log out or shut down their computers when away from their desk;

(e) visitors who require access to data importer's facilities must enter through a staffed and/or main facility entrance. Visitors must register their date and time of arrival, time of leaving the building and the name of the person they are visiting. Visitors must produce a current, government issued form of identification to validate their identity. To prevent access to, or disclosure of, company proprietary information visitors are not allowed un-escorted access to restricted or controlled areas;

(f) select data importer facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted;

(g) locked shred bins are provided on most sites to enable secure destruction of confidential information/personal data;

(h) for data importer's major data centres, security guards, UPS and generators, and change control standards are available;

(i) for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a data classification program to manage risk arising from such activities.

CHANGE MANAGEMENT. The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

SECURITY INCIDENTS AND RESPONSE PLAN

1. **Security incident response plan:** Data importer maintains a security incident response policy and related plan and procedures which address the measures that data importer will take in the event of loss of control, theft, unauthorized disclosure, unauthorized access, or unauthorized acquisition of personal data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. **Response controls:** Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to the data importer's IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

DATA TRANSMISSION CONTROL AND ENCRYPTION. Data importer shall, to the extent it has control over any electronic transmission or transfer of personal data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered or removed without proper authority during its transmission or transfer. In particular, data importer shall:

1. implement industry-standard encryption practices in its transmission of personal data. Industry-standard encryption methods used by data importer includes Secure Sockets Layer (SSL), Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec);

2. if technically feasible, encrypt all personal data, including, in particular any sensitive personal data or confidential information, when transmitting or transferring that data over any public network, or over any network not owned and maintained by data importer. The data importer's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document;

3. for Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on a network that contains such information (including data importer's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

SYSTEM ACCESS CONTROLS. Access to data importer's systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted so as to prevent access from unauthorised individuals. Such procedures include:

1. **admission controls** (i.e. measures to prevent unauthorized persons from using data processing systems):
   (a) access is provided based on segregation of duties and least privileges in order to reduce the risk of misuse, intention or otherwise;

(b) access to IT systems will be granted only when a user is registered under a valid username and password;

(c) data importer has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;

(d) mandatory password changes on a regular basis;

(e) automatic computer lock, renewed access to the PC only after new registration with a valid username and password;

(f) data and user classification determines the type of authentication that must be used by each system;

(g) remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. **access controls** (i.e. measures to prevent unauthorised access to systems):

(a) access authorization is issued in respect of the specific area of work the individual is assigned to (i.e. work role);

(b) adjustment of access authorizations in case of changes to the working area, or in case an employee's employment is terminated for any reason;

(c) granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question;

(d) event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

DATA ACCESS CONTROL. Data importer applies the controls set out below regarding the access and use of personal data:

1. personnel are instructed to only use the minimum amount of personal data necessary in order to achieve the data importer's relevant business purposes
2. personnel are instructed not to read, copy, modify or remove personal data unless necessary in order to carry out their work duties;
3. third party use of personal data is governed through contractual terms and conditions between the third party and data importer which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services;

SEPARATION CONTROL. Where legally required, data importer will ensure that personal data collected for different purposes can be processed separately. Data importer shall also ensure there is separation between test and production systems.

AVAILABILITY CONTROL. Data importer protects personal data against accidental destruction or loss by following these controls:

1. personal data is retained in accordance with customer contract or, in its absence, data importer's record management policy and practices, as well as legal retention requirements;
2. hardcopy personal data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;
3. electronic personal data is given to data importer's IT Asset Management team for proper disposal;
4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms.

DATA INPUT CONTROL. Data importer has, where appropriate, measures designed to check whether and by whom personal data have been input into data processing systems, or whether such data has been modified or removed. Access to relevant applications is recorded.

SYSTEM DEVELOPMENT AND MAINTENANCE. Publicly released third party vulnerabilities are reviewed for applicability in the data importer environment. Based on risk to data importer's business and customers, there are pre-determined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

COMPLIANCE. The information security, legal, privacy and compliance departments work to identify regional laws and regulations that may be applicable to data importer. These requirements cover areas such as, intellectual property of the data importer and its customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements. Mechanisms such as the information security program, the executive privacy council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors included on a list provided by processor and incorporated by reference into these EU Standard Contractual Clauses – Controller to Processor as of their effective date.

EU STANDARD CONTRACTUAL CLAUSES - PROCESSOR TO CONTROLLER

For the purpose of EU Standard Contractual Clauses – Processor to Controller, the data exporting organization is the Provider under the Data Processing Agreement, and the data importing organization is Dell Products, an unlimited company organized under the laws of Ireland with registered number 191034 and whose registered office is at 70 Sir John Rogerson's Quay, Dublin 2, Ireland together with all other Dell group entities (as defined below), each such Dell entity having the right to enforce the terms of these Standard Contractual Clauses as a third party beneficiary against the data importer in respect of any personal data which are processed by such Dell entity as a controller, as if such Dell entity were entering into its own separate set of Standard Contractual Clauses with the data importer.

Dell group entity means a party or any business entity at any time controlling, controlled by or under common control with Dell Products. "**Control**" means in respect of a company, the power of a person to directly or indirectly secure that the affairs of the company are conducted in accordance with the wishes or directions of that person. "Controlling", "controlled by" and "under common control" shall be construed accordingly.

SECTION I

***CLAUSE 1*: PURPOSE AND SCOPE**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([ii]) for the transfer of personal data to a third country.

(b) The Parties:
   (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
   (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

   have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

***CLAUSE 2:* EFFECT AND INVARIABILITY OF THE CLAUSES**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

***CLAUSE 3:* THIRD-PARTY BENEFICIARIES**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   (ii) Clause 8.1 (b) and Clause 8.3(b);
   (iii) N/A
   (iv) N/A
   (v) Clause 13;
   (vi) Clause 15.1(c), (d) and (e);
   (vii) Clause 16(e);
   (viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

***CLAUSE 4:* INTERPRETATION**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***CLAUSE 5:* HIERARCHY** In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

***CLAUSE 6:* DESCRIPTION OF THE TRANSFER(S)** The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***CLAUSE 7:* DOCKING CLAUSE – Intentionally omitted.**

SECTION II – OBLIGATIONS OF THE PARTIES

***CLAUSE 8:* DATA PROTECTION SAFEGUARDS** The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (iii), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

CLAUSE 9: **USE OF SUB-PROCESSORS** Not applicable; intentionally omitted.

CLAUSE 10: **DATA SUBJECT RIGHTS** The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

CLAUSE 11: **REDRESS**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

CLAUSE 12: **LIABILITY**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

CLAUSE 13**: SUPERVISION** Not applicable; intentionally omitted.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 14: **LOCAL LAWS AND PRACTICES AFFECTING COMPLIANCE WITH THE CLAUSES**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (iv);

  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 15: **OBLIGATIONS OF THE DATA IMPORTER IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

  (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

  (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

CLAUSE 16: **NON-COMPLIANCE WITH THE CLAUSES AND TERMINATION**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    (ii) the data importer is in substantial or persistent breach of these Clauses; or
    (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

***CLAUSE 17*: GOVERNING LAW** These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

***CLAUSE 18*: CHOICE OF FORUM AND JURISDICTION** Any dispute arising from these Clauses shall be resolved by the courts of Ireland.

ANNEX I – PROCESSOR TO CONTROLLER

A. LIST OF PARTIES

DATA EXPORTER. The data exporter is identified at the start of the Clauses and is a provider of IT products and services. The data exporter has appointed the data importer to provide certain products and/or services as specified in the Provider Agreement. To facilitate the provision of these products and services, the data exporter may provide to the data importer access to the personal data described in Section B, -below. The data exporter's contact for data protection (its data protection officer and/or representative in the European Union) may be reached at the address provided in the Data Protection Agreement.

DATA IMPORTER. The data importer is a signatory to the Clauses and a provider of products and/or services, and whose data protection officer may be reached by sending an email to privacy@dell.com. The data importer will be the recipient of personal data which is exported by the data exporter to the data importer as described below.

B. DESCRIPTION OF TRANSFER

DATA SUBJECTS. The personal data transferred may concern the following categories of data subjects:

- Past, present and prospective employees and partners;
- Past, present and prospective clients, customers, end users, web site visitors;
- Past, present and prospective advisors, consultants, suppliers, contractors, subcontractors and agents;
- Beneficiaries and relatives.

CATEGORIES OF DATA. The data subjects' personal data transferred may concern the following categories of data:

1. Contact details (which may include name, address, e-mail address, phone and fax contact details and associated local time zone information);
2. Employment details (which may include company name, job title, grade, demographic and location data);
3. IT systems information (which may include user ID and password, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies);
4. Data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails);
5. Details of goods or services provided to or for the benefit of data subjects;
6. Financial details (e.g. credit, payment and bank details).

SPECIAL CATEGORIES OF DATA (IF APPROPRIATE). Personal data transferred may include information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union opinions, memberships or activities, social security files, and data concerning health (including physical or mental health or condition), sexual life and information regarding criminal offences or alleged offences and any related court proceedings and shall include special categories of data as defined in Article 8 of the Directive 95/46/EC.

PROCESSING OPERATIONS. The personal data transferred may be subject to the following processing activities: Any operation with regard to personal data irrespective of the means applied and procedures, in particular the obtaining, collecting, recording, organizing, storage, holding, use, amendment, adaptation, alteration, disclosure, dissemination or otherwise making available, aligning, combining, retrieval, consultation, archiving, transmission, blocking, erasing, or destruction of data, the operation and maintenance of systems, management and management reporting, financial reporting, risk management, compliance, legal and audit functions and shall include "processing" which shall have the meaning given to such term in the Directive.

TRANSFER DETAILS. The frequency of the transfer (e.g., whether the data will be transferred on a one-off or continuous basis), purpose of the data transfer and further processing, period for which the personal data will be retained or the criteria used to determine that period and details concerning any transfers to sub-processors will be as set forth in the corresponding product or services agreement to which these standard contractual clauses relate.

UK STANDARD CONTRACTUAL CLAUSES

These Clauses are attached to and made a part of the Data Protection Agreement ("**DPA**") between Dell and Provider, and apply where any Dell entity named in the master agreement located in the United Kingdom may serve as a data exporter, as defined below. Such Dell entity, together with all other Dell group entities (as defined below), each such Dell entity having the right to enforce the terms of these Standard Contractual Clauses as a third party beneficiary against the data importer in respect of any personal data which are processed by such Dell entity as a controller, as if such Dell entity were entering into its own separate set of Standard Contractual Clauses with the data importer.

Dell group entity means a party or any business entity at any time controlling, controlled by or under common control with Dell Products. "**Control**" means in respect of a company, the power of a person to directly or indirectly secure that the affairs of the company are conducted in accordance with the wishes or directions of that person. "Controlling", "controlled by" and "under common control" shall be construed accordingly.

1) ***CLAUSE 1*** **DEFINITIONS**. For the purposes of the Clauses:

   a) **'personal data'**, '**special categories of data'**, '**process/processing'**, '**controller'**, '**processor'**, '**data subject'** and '**supervisory authority'** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

   b) **"the data exporter"** shall mean the controller who transfers the personal data;

   c) **"the data importer"** shall mean the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of these Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

   d) **"the sub-processor"** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

   e) **"the applicable data protection law"** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

   f) **"technical and organizational security measures"** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2) ***CLAUSE 2*** **DETAILS OF THE TRANSFER.** The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3) ***CLAUSE 3*** **THIRD-PARTY BENEFICIARY CLAUSE**

   1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

   2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

   3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

   4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4) ***CLAUSE 4*** **OBLIGATIONS OF THE DATA EXPORTER.** The data exporter agrees and warrants:

   a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

   b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

   c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to these Clauses;

d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e) that it will ensure compliance with the security measures;

f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

5) ***CLAUSE 5*** **OBLIGATIONS OF THE DATA IMPORTER.** The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

d) that it will promptly notify the data exporter about:

i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

ii) any accidental or unauthorized access; and

iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i) that the processing services by the sub-processor will be carried out in accordance with Clause 11 (Sub-processing);

j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6) ***CLAUSE 6*** **LIABILITY**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has

assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7) ***CLAUSE 7*** **MEDIATION AND JURISDICTION**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   b. to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8) ***CLAUSE 8*** **COOPERATION WITH SUPERVISORY AUTHORITIES**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9) ***CLAUSE 9*** **GOVERNING LAW.** The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10) ***CLAUSE 10*** **VARIATION OF THE CONTRACT.** The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

11) ***CLAUSE 11*** **SUB-PROCESSING**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12) ***CLAUSE 12*** **OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA-PROCESSING SERVICES**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon the request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

These Clauses are attached to and made a part of the Data Protection Agreement ("**DPA**") between Dell and Provider. This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

DATA EXPORTER. The data exporter is identified at the start of the Clauses and is a provider of IT products and services. The data exporter has appointed the data importer to provide certain products and/or services as specified in the Provider Agreement. To facilitate the provision of these products and services, the data exporter may provide to the data importer access to the personal data described below.

DATA IMPORTER. The data importer is a signatory to the Clauses and a provider of products and/or services. The data importer will be the recipient of personal data which is exported by the data exporter to the data importer as described below.

DATA SUBJECTS. The personal data transferred may concern the following categories of data subjects:

- Past, present and prospective employees and partners;
- Past, present and prospective clients, customers, end users, web site visitors;
- Past, present and prospective advisors, consultants, suppliers, contractors, subcontractors and agents;
- Beneficiaries and relatives.

CATEGORIES OF DATA. The data subjects' personal data transferred may concern the following categories of data:

1. Contact details (which may include name, address, e-mail address, phone and fax contact details and associated local time zone information);
2. Employment details (which may include company name, job title, grade, demographic and location data);
3. IT systems information (which may include user ID and password, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies);
4. Data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails);
5. Details of goods or services provided to or for the benefit of data subjects;
6. Financial details (e.g. credit, payment and bank details).

SPECIAL CATEGORIES OF DATA (IF APPROPRIATE). Personal data transferred may include information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union opinions, memberships or activities, social security files, and data concerning health (including physical or mental health or condition), sexual life and information regarding criminal offences or alleged offences and any related court proceedings and shall include special categories of data as defined in Article 8 of the Directive 95/46/EC.

PROCESSING OPERATIONS. The personal data transferred may be subject to the following processing activities: Any operation with regard to personal data irrespective of the means applied and procedures, in particular the obtaining, collecting, recording, organizing, storage, holding, use, amendment, adaptation, alteration, disclosure, dissemination or otherwise making available, aligning, combining, retrieval, consultation, archiving, transmission, blocking, erasing, or destruction of data, the operation and maintenance of systems, management and management reporting, financial reporting, risk management, compliance, legal and audit functions and shall include "processing" which shall have the meaning given to such term in the Directive.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES
Data Importer Information Security Overview

These Clauses are attached to and made a part of the Data Protection Agreement ("**DPA**") between Dell and Provider. This Appendix 2 sets out a description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c). Data importer takes information security seriously and this approach is followed through in its processing and transfers of personal data. This information security overview applies to data importer's corporate controls for safeguarding personal data which is processed and transferred amongst the data importer's group companies. Data importer's information security program enables the workforce to understand their responsibilities. Some customer solutions may have alternate safeguards outlined in the applicable statement of work as agreed with each customer.

SECURITY PRACTICES. Data importer has implemented corporate information security practices and standards that are designed to safeguard data importer's corporate environment and to address business objectives across the following areas: (1) information security, (2) system and asset management, (3) development, and (4) governance. These practices and standards are approved by the data importer's executive management and are periodically reviewed and updated where necessary. Data importer shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data and sensitive personal data throughout its lifecycle. Key policies should be reviewed at least annually.

ORGANIZATIONAL SECURITY. It is the responsibility of the individuals across the data importer's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, data importer's Information Security ("**IS**") function is responsible for the following activities:

1. **Security strategy** – the IS function drives data importer's security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS function also carries out risk assessments and risk management activities, and manages contract security requirements.
2. **Security engineering** – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.
3. **Security operations** – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.
4. **Forensic investigations** – the IS function works with Security Operations, Legal, Global Privacy Office and Human Resources to carry out investigations, including eDiscovery and eForensics.
5. **Security consulting and testing** – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

ASSET CLASSIFICATION AND CONTROL. Data importer's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that data importer might track include:

- information assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information
- software assets, such as identified applications and system software
- physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

EMPLOYEE SCREENING, TRAINING AND SECURITY

1. **Screening/background checks:** Where reasonably practicable and appropriate, as part of the employment/recruitment process, data importer shall perform screening/background checks on employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to data importer's networks, systems or facilities.
2. **Identification:** Data importer shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other data importer entities or customers for whom the employee is providing services.
3. **Training:** Data importer's annual compliance training program includes a requirement for employees to complete a data protection and information security awareness course and pass an assessment at the end of the course. The security awareness course may also provide materials specific to certain job functions.
4. **Confidentiality:** Data importer shall ensure its employees are legally bound to protect and maintain the confidentiality of any personal data they handle pursuant to standard agreements.

PHYSICAL ACCESS CONTROLS AND ENVIRONMENTAL SECURITY

1. **Physical Security Program:** Data importer shall use a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably practicable. Data importer's security team works closely with each site to determine appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which personal data is processed and continually monitor any changes to the physical infrastructure, business and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniqueness in business practice and expectations of data importer. Data importer balances its approach towards security by considering elements of control that include architecture, operations and systems.
2. **Physical Access controls:** Physical access controls/security measures at data importer's facilities/premises are designed to meet the following requirements:

(a) access to data importer's buildings, facilities and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to the data importer. Only personnel associated with data importer are provided access to data importer's facilities and physical resources in a manner consistent with their role and responsibilities in the organization;

(b) relevant data importer facilities are secured by an access control system. Access to such facilities is granted with an activated card only;

(c) all persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g. a badge or keycard assigned to one individual) by the IS function. Individuals issued with unique physical access credentials are instructed not to allow or enable other individuals to access the data importer's facilities or resources using their unique credentials (e.g. no "tailgating"). Temporary (up to 14 days) credentials may be issued to individuals who do not have active identities where this is necessary (i) for access to a specific facility and (ii) for valid business needs. Unique credentials are non-transferable and if an individual cannot produce their credentials upon request they may be denied entry to data importer's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative;

(d) employees are regularly trained and reminded to always carry their credentials, store their laptops, portable devices and documents in a secure location (especially while traveling) and log out or shut down their computers when away from their desk;

(e) visitors who require access to data importer's facilities must enter through a staffed and/or main facility entrance. Visitors must register their date and time of arrival, time of leaving the building and the name of the person they are visiting. Visitors must produce a current, government issued form of identification to validate their identity. To prevent access to, or disclosure of, company proprietary information visitors are not allowed un-escorted access to restricted or controlled areas;

(f) select data importer facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted;

(g) locked shred bins are provided on most sites to enable secure destruction of confidential information/personal data;

(h) for data importer's major data centres, security guards, UPS and generators, and change control standards are available;

(i) for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a data classification program to manage risk arising from such activities.

CHANGE MANAGEMENT. The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

SECURITY INCIDENTS AND RESPONSE PLAN

1. **Security incident response plan:** Data importer maintains a security incident response policy and related plan and procedures which address the measures that data importer will take in the event of loss of control, theft, unauthorized disclosure, unauthorized access, or unauthorized acquisition of personal data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. **Response controls:** Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to the data importer's IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

DATA TRANSMISSION CONTROL AND ENCRYPTION. Data importer shall, to the extent it has control over any electronic transmission or transfer of personal data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered or removed without proper authority during its transmission or transfer. In particular, data importer shall:

1. implement industry-standard encryption practices in its transmission of personal data. Industry-standard encryption methods used by data importer includes Secure Sockets Layer (SSL), Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec);

2. if technically feasible, encrypt all personal data, including, in particular any sensitive personal data or confidential information, when transmitting or transferring that data over any public network, or over any network not owned and maintained by data importer. The data importer's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document;

3. for Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on a network that contains such information (including data importer's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

SYSTEM ACCESS CONTROLS. Access to data importer's systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted so as to prevent access from unauthorised individuals. Such procedures include:

1. **admission controls** (i.e. measures to prevent unauthorized persons from using data processing systems):
   (a) access is provided based on segregation of duties and least privileges in order to reduce the risk of misuse, intention or otherwise;
   (b) access to IT systems will be granted only when a user is registered under a valid username and password;
   (c) data importer has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;
   (d) mandatory password changes on a regular basis;
   (e) automatic computer lock, renewed access to the PC only after new registration with a valid username and password;
   (f) data and user classification determines the type of authentication that must be used by each system;

(g) remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. **access controls** (i.e. measures to prevent unauthorised access to systems):

(a) access authorization is issued in respect of the specific area of work the individual is assigned to (i.e. work role);

(b) adjustment of access authorizations in case of changes to the working area, or in case an employee's employment is terminated for any reason;

(c) granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question;

(d) event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

DATA ACCESS CONTROL. Data importer applies the controls set out below regarding the access and use of personal data:

1. personnel are instructed to only use the minimum amount of personal data necessary in order to achieve the data importer's relevant business purposes
2. personnel are instructed not to read, copy, modify or remove personal data unless necessary in order to carry out their work duties;
3. third party use of personal data is governed through contractual terms and conditions between the third party and data importer which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services;

SEPARATION CONTROL. Where legally required, data importer will ensure that personal data collected for different purposes can be processed separately. Data importer shall also ensure there is separation between test and production systems.

AVAILABILITY CONTROL. Data importer protects personal data against accidental destruction or loss by following these controls:

1. personal data is retained in accordance with customer contract or, in its absence, data importer's record management policy and practices, as well as legal retention requirements;
2. hardcopy personal data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;
3. electronic personal data is given to data importer's IT Asset Management team for proper disposal;
4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms.

DATA INPUT CONTROL. Data importer has, where appropriate, measures designed to check whether and by whom personal data have been input into data processing systems, or whether such data has been modified or removed. Access to relevant applications is recorded.

SYSTEM DEVELOPMENT AND MAINTENANCE. Publicly released third party vulnerabilities are reviewed for applicability in the data importer environment. Based on risk to data importer's business and customers, there are pre-determined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

COMPLIANCE. The information security, legal, privacy and compliance departments work to identify regional laws and regulations that may be applicable to data importer. These requirements cover areas such as, intellectual property of the data importer and its customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements. Mechanisms such as the information security program, the executive privacy council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

US HIPAA SUBCONTRACTOR AGREEMENT

Dell Inc. and its worldwide direct and indirect subsidiaries ("**Dell**" or "**Business Associate**") and Provider, its parent company and its worldwide direct and indirect subsidiaries ("**Subcontractor**") entered into an agreement pursuant to which Dell purchases products from Provider and Provider performs services on Dell's behalf ("**Provider Agreement**"). This HIPAA Subcontractor Agreement ("**HIPAA Agreement**") is attached to and made a part of the Data Protection Agreement ("**DPA**") between Dell and Subcontractor.

1. **STATEMENT OF PURPOSE.** DELL HAS BEEN ENGAGED TO PROVIDE CERTAIN SERVICES TO ITS CUSTOMERS. IN CONNECTION WITH THESE ENGAGEMENTS, DELL HAS ENTERED INTO BUSINESS ASSOCIATE AGREEMENTS WITH CERTAIN OF ITS CUSTOMERS AS REQUIRED BY THE PRIVACY AND SECURITY RULES OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("**HIPAA**"). DELL IS NOW ENTERING INTO THIS HIPAA AGREEMENT WITH SUBCONTRACTOR IN CONNECTION WITH DELL SUBCONTRACTING ALL OR A PART OF THE PERFORMANCE OF SUCH SERVICES TO SUBCONTRACTOR PURSUANT TO THE PROVIDER AGREEMENT(S). THE PARTIES ACKNOWLEDGE THAT SUBCONTRACTOR MAY BE RESPONSIBLE FOR FACILITIES OR SYSTEMS THAT HOUSE OR CONTAIN PHI, AND/OR MAY BE EXPOSED TO, CREATE, RECEIVE, MAINTAIN, TRANSMIT OR BECOME AWARE OF PHI IN THE PERFORMANCE OF THE SERVICES UNDER THE PROVIDER AGREEMENT(S) BETWEEN DELL AND SUBCONTRACTOR. THIS HIPAA AGREEMENT CONSTITUTES THE WRITTEN ASSURANCES REQUIRED BY THE HIPAA RULES IN CONNECTION WITH SUBCONTRACTOR'S ACTIVITIES UNDER THIS HIPAA AGREEMENT AND THE PROVIDER AGREEMENT(S).
2. **ORDER OF PRECEDENCE.** In the event that a provision of this HIPAA Agreement is contrary to a provision of a Provider Agreement, the provision of this HIPAA Agreement shall control. Any ambiguity in the terms of this HIPAA Agreement will be resolved to permit Dell and Dell's Customers to comply with HIPAA. Nothing in this HIPAA Agreement shall change or modify any terms of the Provider Agreement(s) that prohibit Subcontractor from retaining subcontractors or agents to assist in the performance of Services for Dell.
3. **DEFINITIONS**. Capitalized terms not specifically defined in this HIPAA Agreement have the meanings set forth in the DPA, the NDA, or the applicable Provider Agreement.
   - 3.1. "**Breach**" has the meaning set forth in 45 C.F.R. § 164.402.
   - 3.2. "**Covered Entity**" has the meaning set forth in 45 C.F.R. § 160.103.
   - 3.3. "**Customers**" means customers of Dell who are Covered Entities under HIPAA.
   - 3.4. "**Data Aggregation**" has the meaning set forth in 45 C.F.R. § 164.501.
   - 3.5. "**Designated Record Set**" has the meaning set forth in 45 C.F.R. Section 164.501.
   - 3.6. "**Discovery**" means "discovery" as such term is described in 45 C.F.R. § 164.410(a)(2).
   - 3.7. "**ePHI**" means "Electronic Protected Health Information" as defined in 45 C.F.R. § 160.103 that is created, received, maintained or transmitted by Subcontractor from or on behalf of Dell or Dell's Customers under the Provider Agreement(s).
   - 3.8. "**HIPAA Breach Notification Rule**" means the Notification in the Case of Breach of Unsecured Protected Health Information, as set forth at 45 C.F.R. Part 164 Subpart D.
   - 3.9. "**HIPAA Privacy Rule**" means the standards, requirements and specifications promulgated by at 45 C.F.R. Section 160 subparts A and E promulgated under HIPAA.
   - 3.10. "**HIPAA Security Rule**" means the standards, requirements and specifications promulgated by the Secretary at 45 C.F.R. Section 164 subpart C promulgated under HIPAA.
   - 3.11. "**HIPAA Rules**" means the HIPAA Privacy Rule, the HIPAA Security Rules, the Breach Notification Rule, as the same may, from time to time, be amended.
   - 3.12. "**Individual"** has the meaning set forth in 45 C.F.R. § 160.103.
   - 3.13. "**PHI**" means "Protected Health Information" as defined in 45 C.F.R. § 164.501 that is created, received, maintained or transmitted by Subcontractor from or on behalf of Dell or Dell's Customers under the Provider Agreement(s).
   - 3.14. "**Required by Law**" has the meaning set forth in 45 C.F.R. § 164.103.
   - 3.15. "**Secretary**" has the meaning set forth in 45 C.F.R. § 160.103.
   - 3.16. "**Security Incident**" has the meaning set forth in 45 C.F.R. § 164.304.
   - 3.17. "**Sell**" or "**Sale**" means a disclosure of PHI by Subcontractor where Subcontractor directly or indirectly receives remuneration from or on behalf of the recipient of such PHI in exchange for such PHI, but does not include any disclosure of PHI described in 45 C.F.R. § 164.502(a)(5)(ii)(B)(2).
   - 3.18. "**Unsecured Protected Health Information**" shall have the meaning set forth in 45 C.F.R. § 164.402.
4. **OBLIGATIONS OF SUBCONTRACTOR.** Subcontractor agrees:
   - 4.1. not to use or further disclose PHI other than as required to carry out its obligations to Dell under the Provider Agreement(s) and as expressly permitted or required by this HIPAA Agreement or as Required by Law. Such use, disclosure or request of PHI shall utilize a limited data set if practicable or otherwise the minimum necessary PHI to accomplish the intended purpose of the use, disclosure or request;
   - 4.2. to use reasonable and appropriate safeguards to prevent the use or disclosure of PHI in any manner other than as permitted by this HIPAA Agreement, consistent with the applicable principles and obligations set out in the HIPAA Rules;
   - 4.3. to report to Dell in writing any use or disclosure of PHI not provided for by this HIPAA Agreement of which it becomes aware within 24 hours of becoming aware of such use or disclosure. In addition, Subcontractor will report to Dell in writing, within 24 hours following Discovery, any acquisition, access, use, or disclosure of Unsecured Protected Health Information, unless such event is excluded from the definition of Breach in 45 C.F.R. § 164.402(1). Any such report shall include the identification (if known) of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business

Associate to have been, accessed, acquired, or disclosed, all other information required by 45 C.F.R. § 164.410(c), and any other information reasonably requested by Dell or the applicable Customer. Upon receipt of such report, Dell will then conduct, or have Subcontractor conduct at Dell's direction, a risk assessment to determine whether such acquisition, access, use, or disclosure compromised the security or privacy of such Unsecured Protected Health Information based on the factors specified in the definition of Breach in 45 C.F.R. § 164.402(2). If Subcontractor believes, based on such risk assessment, that any such acquisition, access, use, or disclosure results in a low probability that the Unsecured Protected Health Information has been compromised, it shall provide to Dell all information supporting such conclusion;

4.4. to ensure, in accordance with 164.502(e)(1)(ii) and 164.504(e)(2)(ii)(D), that any agents or subcontractors who create, receive, maintain or transmit PHI agree to provide reasonable assurances, evidenced by written contract, that such agents or subcontractors will comply with substantially the same restrictions and conditions that apply to Subcontractor with respect to such information;

4.5. to the extent (if any) that Subcontractor maintains a Designated Record Set, to make available PHI maintained by Subcontractor in a Designated Record Set to Dell as required for Dell's Customers to comply with their obligation to give an Individual the right of access to inspect and obtain a copy of their PHI as set forth in 45 C.F.R. § 164.524. If specifically requested by Dell or the applicable Customer, Subcontractor will:

(a) Electronic Copies. Transmit copies of the PHI in an electronic format directly to a person the Individual designates.

(b) Paper Copies. Make copies of the PHI in a paper form and provide such copies directly to a person the Individual designates.

4.6. to the extent (if any) that Subcontractor maintains a Designated Record Set, to make available PHI maintained by Subcontractor in a Designated Record Set to Dell as required for Dell's Customers to comply with their obligation to amend PHI as set forth in 45 CFR 164.526;

4.7. to make available to Dell information regarding disclosures of PHI by Subcontractor for which an accounting is required under 45 C.F.R. Section 164.528 so Dell's Customers can meet their requirements to provide an accounting of disclosures to Individuals in accordance with 45 CFR 164.528;

4.8. to make its internal practices, books and records relating to its compliance with its obligations under this HIPAA Agreement and the use and disclosure of PHI by Subcontractor available to the Secretary for purposes of determining Dell or Dell's Customers' compliance with the HIPAA Rules, and to provide any such materials to Dell or Dell's Customer upon request;

4.9. in accordance with 45 C.F.R. § 164.502(a)(4)(i), to disclose PHI when required by the Secretary under subpart C of part 160 of HIPAA;

4.10. at termination of this HIPAA Agreement for any reason, if feasible, return, or at Dell's election destroy, all PHI that Subcontractor still maintains in any form and to retain no copies of such information, or, if such return or destruction is not feasible, Subcontractor shall (i) provide Dell with notification of the conditions that make return or destruction infeasible, (ii) extend the protections of this HIPAA Agreement to the PHI, and (iii) limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. If Dell elects the destruction of such PHI, certify to Dell in writing that such destruction has occurred;

4.11. With respect to ePHI, to:

(a) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI, as required by the Security Rule, including the applicable administrative, physical and technical safeguards described in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314 and 45 C.F.R. § 164.316 with respect to ePHI to prevent the use or disclosure of ePHI other than as provided in this HIPAA Agreement; provided, however, Subcontractor shall encrypt ePHI in transit and at rest in accordance with Section 3(f) of the DPA, unless (A) Subcontractor (1) determines that such encryption is not reasonable and appropriate via a risk assessment conducted and documented by Subcontractor in accordance with applicable HIPAA provisions, and (B) provides a copy of such documentation to Dell; and (C) Dell provides Subcontractor with written approval of any such non-encryption.

(b) ensure, in accordance with 45 C.F.R. §§ 164.504(e)(2)(ii)(D), 164.308(b)(2) and (3) and 164.314(a)(2)(iii), that any agent, including a subcontractor, who create, receive, maintain or transmit ePHI agrees, evidenced by written contract, to implement reasonable and appropriate safeguards to protect such ePHI consistent with the requirements described in clause (i) of this Section 3(j); and

(c) report to Dell any Security Incident affecting ePHI of which it becomes aware;

4.12. not to Sell PHI;

4.13. mitigate, to the extent practicable, any harmful effect that is known to Subcontractor of a use or disclosure of PHI by Subcontractor in violation of this HIPAA Agreement;

4.14. not to perform Data Aggregation activities nor de-identify PHI unless specifically requested in writing by Dell;

4.15. to reimburse Dell for the costs it incurs in responding to (including providing notifications and credit monitoring services), remediating, and/or mitigating damages caused by a Breach of Unsecured Protected Health Information or a Security Incident caused by Subcontractor's failure to perform its obligations under this HIPAA Agreement, the DPA, the NDA, or the Provider Agreement or a use of disclosure of PHI by Subcontractor not provided for by this HIPAA Agreement, and the costs Dell incurs in following up a complaint by an Individual or a regulator related to the foregoing; and

4.16. to comply with any (i) modifications to, restrictions on, defects in, or revocation or other termination of the effectiveness of, any consent, authorization or permission relating to the use or disclosure of PHI; and (ii) agreement that Dell or the applicable Customer makes or limitations in the applicable Customer's privacy practices that either (A) restricts the use or disclosure of PHI pursuant to 45 C.F.R. § 164.522(a) or 45 C.F.R. § 164.520, or (B) requires confidential communication about PHI pursuant to 45 C.F.R. § 164.522(b), in each case under clause (i) or (ii), to the extent any such modification, defect, revocation,

termination, restriction, confidential communication obligations or limitations affect Subcontractor's permitted or required uses and disclosures of PHI specified in this HIPAA Agreement (collectively, "**Restrictions**"), provided that Dell or the applicable Customer notifies Subcontractor in the Restrictions that Subcontractor must follow.

5. **TERM AND TERMINATION.** With respect to each Provider Agreement, the term of this HIPAA Agreement shall be the same as the term of such Provider Agreement. Upon Dell's knowledge of a material breach of this HIPAA Agreement by Subcontractor, or Subcontractor's knowledge of such breach, which shall be promptly disclosed to Dell, Dell may in Dell's discretion, provide an opportunity for Subcontractor to cure the breach or end the violation within thirty (30) business days of such notification. If Subcontractor fails to cure the breach or end the violation within such time period to the satisfaction of Dell, or Dell in its own discretion does not provide such an opportunity, Dell shall have the right to immediately terminate this HIPAA Agreement and the Agreement(s) that are the subject of such breach upon written notice to Subcontractor. In the event that termination of such Agreement(s) is not feasible in Dell's discretion, Subcontractor hereby acknowledges that Dell shall have the right to report the breach to the Secretary.
6. **SUBCONTRACTORS.** Subcontractor acknowledges that to the extent required by HIPAA (e.g., 45 C.F.R. §§ 160.102(b), 160.300, 164.104(b), 164.302, and 164.500(c)) the standards and requirements of the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rule apply to Subcontractor.
7. **INDEMNIFICATION.** Subcontractor shall indemnify, hold harmless and defend Dell and Dell's directors, officers, employees, representatives, and agents from and against any and all claims, actions, demands, and legal proceedings and all liabilities, damages, losses, judgments, authorized settlements, costs, fines, penalties and expenses including reasonable attorneys' fees arising out of or in connection with, resulting from or relating to the acts or omissions of Subcontractor in connection with a breach of the representations, duties and obligations of Subcontractor under this HIPAA Agreement or Subcontractor's violation of the HIPAA Rules.

BUSINESS ASSOCIATE AGREEMENT

Dell Inc. and its worldwide direct and indirect subsidiaries, in its capacity as Plan Sponsor ("**Plan Sponsor**") of the Dell Inc. Comprehensive Welfare Benefits Plan ("**Plan**") has engaged Provider to provide certain professional, consulting or other services to the Plan (the "**Services**") pursuant to an agreement (the "**Provider Agreement**"). This Business Associate Agreement ("**BAA Agreement**") is attached to and made a part of the Data Protection Agreement ("**DPA**") between Dell and Provider.

1. **STATEMENT OF PURPOSE.** Because Provider may access, retain, be exposed to, or become aware of confidential health information of participants of Plan in the performance of the Services, the parties agree to protect the confidentiality of such information in accordance with federal and state laws and regulations including, but not limited to, information protected by the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), the Health information Technology for Economic and Clinical Health Act ("**HITECH Act**"), and the regulations promulgated thereto ("**HIPAA Regulations**"), including, as amended from time to time, (a) the standards, requirements and specifications promulgated by the Secretary at 45 C.F.R. Part 164 subparts A and E ("**Privacy Rule**"); (b) the security standards published on February 20, 2003 at Fed. Reg. 8334 et. seq. (45 C.F.R. Parts 160, 162 and 164) ("**HIPAA Security Rule**"); and (c) the breach notification standards, requirements, and specifications enacted by Subtitle D of the HITECH Act and its implementing regulations promulgated by the Secretary at 45 C.F.R. Part 164 Subpart D as part of the final omnibus rule ("**Omnibus Rule**") (collectively, "**Breach Notification Rule**"); and (d) the enforcement standards, requirements and specifications promulgated by the Secretary at 45 C.F.R. Part 160 subparts C, D, and E ("**Enforcement Rule**").

2. **DEFINITIONS.** Capitalized terms not specifically defined in this BAA Agreement have the meanings set forth in the DPA, the NDA, the applicable Provider Agreement or the HIPAA Regulations.

   2.1. "**Breach**" means the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI, as defined and subject to the exceptions set forth in 45 C.F.R. § 164.402.

   2.2. "**Discovery**" in relation to the discovery of a Breach, has the meaning set forth in the HITECH Act or other applicable law, including 45 C.F.R. § 164.410(a)(2).

   2.3. **"ePHI"** means "Electronic Protected Health Information" as defined in the HIPAA Security Rule that is created, received, maintained or transmitted by or on behalf of Plan.

   2.4. "**HIPAA Security Rule**" means the Security Standards published at 45 C.F.R. Parts 160, 162 and 164 and as may be amended from time to time.

   2.5. "**HITECH Act**" means the Privacy Provisions of the Health Information Technology for Economic and Clinical Health Act, Sections 13400 et seq. enacted on February 17, 2009 and the implementing regulations including, but not limited to, the "Breach Notification for Unsecured Protected Health Information" regulations published on August 24, 2009 at 74 Fed. Reg. 42740 et seq. and as may be amended from time to time.

   2.6. "**Individual**" has the same meaning as the term "individual" in 45 C.F.R. § 160.103 and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502 (g).

   2.7. "**Law**" means all applicable Federal and State Statutes and all relevant regulations thereunder.

   2.8. "**PHI"** has the same meaning as the term "Protected Health Information" in 45 C.F.R. § 160.103, limited to the information created, received, maintained, or transmitted by Provider from or on behalf of Plan.

   2.9. "**Secretary**" means the Secretary of the Department of Health and Human Services, or his designee.

   2.10. "**Subcontractor**" means a person or entity to whom Provider delegates a function, activity, or service other than in the capacity of a member of the workforce of Provider.

3. **CONFIDENTIALITY.** Provider recognizes the sensitive and confidential nature of the PHI and agrees (a) that such PHI will be used or disclosed, including the uses and disclosures inherent in the performance of the Services which are generally listed on Exhibit B attached hereto, solely as required or permitted under this BAA Agreement and in accordance with Law or as required by Law; and (b) that Provider shall use reasonable safeguards designed to ensure that the transmission, handling, storage, and use of such PHI by Provider will preserve the confidentiality of the PHI, in accordance with Law including the HIPAA Regulations.

4. **RESPONSIBILITIES OF PROVIDER**

   4.1. Records. Provider will maintain accurate records of all transactions made in connection with this BAA Agreement. Provider acknowledges and agrees to comply with its obligations as a Business Associate under the HIPAA Regulations and all other Law.

   4.2. Accounting. The Plan acknowledges its obligation as a Covered Entity under the Privacy Rule to provide an accounting of disclosures to an Individual in accordance with 45 C.F.R. 164.528. Pursuant to this BAA Agreement and only with respect to PHI, Provider agrees to (i) document and make available to Plan upon request all disclosures of PHI that are subject to an accounting under the Privacy Rule and the HITECH Act, (ii) receive and process requests for accountings from Individuals, (iii) provide accountings to Individuals, and (iv) suspend provision of an accounting, when applicable. Provider will maintain information necessary to provide an accounting for a period of six (6) years from the date of disclosure, unless otherwise required under the HITECH Act and the HIPAA Regulations.

   4.3. Disclosure. Provider agrees to report to Plan within a reasonable timeframe following Discovery of any use or disclosure of information it knows or should know is other than as permitted in this BAA Agreement. To the extent applicable, Provider shall follow the disclosure requirements found in section 5 of this BAA Agreement relating to Breaches of Unsecured PHI.

   4.4. Subcontractors. Provider shall ensure that any agents, including any Subcontractors, who will create, receive, maintain, or transmit any PHI on behalf of Provider agree in writing to the same restrictions, conditions, and requirements relating to the use or disclosure of PHI as required by this BAA Agreement and shall not, in any manner that violates the Privacy Rule or any other applicable provision of law, use or disclose PHI except as set forth in this BAA Agreement. Provider further agrees to ensure that any such agent, including a Subcontractor, to whom it provides EPHI agrees to implement reasonable and

appropriate safeguards to protect such information in accordance with section 4(t) of this BAA Agreement. In the event that Provider discovers a pattern of activity or practice of its Subcontractor that constitutes a material breach or violation of the Subcontractor's obligation under its Provider Agreement, in accordance with 45 C.F.R. § 164.504(e)(1)(iii) and the Omnibus Rule, Provider must take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful, terminate the agreement with the Subcontractor, if feasible.

4.5. Limitations. Provider agrees to limit any request, use and disclosure of PHI, to the extent practicable, to the Limited Data Set or, if needed, to the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure in compliance with the HITECH Act and any regulations or guidance promulgated pursuant thereto. The parties acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the Privacy Rule, HITECH Act and any guidance issued by the Secretary.

4.6. Amendments. The Plan acknowledges its obligation as a Covered Entity under the Privacy Rule to amend an Individual's PHI in accordance with 45 C.F.R. 164.526. Pursuant to this BAA Agreement and with respect to Protected Health Information, Provider agrees to comply with 45 C.F.R. § 164.526, including but not limited to, granting or denying requests for amendment and making amendments to Protected Health Information, when applicable.

4.7. Subpart E Compliance. To the extent the Provider is to carry out one or more of Plan's obligations under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to Plan in the performance of such obligations.

4.8. Practices and Records. Provider agrees to make its internal practices, books and records relating to the use and disclosure of Protected Health Information, including policies and procedures relating to Protected Health Information, received from, or created or received by Provider on behalf of Plan available to Plan and the Secretary for the sole purpose of determining compliance with the HIPAA Regulations.

4.9. Confidentiality. Provider and Plan agree that all confidentiality provisions in this BAA Agreement shall survive termination of this BAA Agreement.

4.10. Data Aggregation. Provider may provide data aggregation services relating to the health care operations of Plan.

4.11. PHI Use. Provider is not prohibited by this BAA Agreement from utilizing PHI for its proper management and administration or to carry out its legal responsibilities, if any. Further, Provider is not prohibited from disclosing PHI for its proper management and administration or to carry out its legal responsibilities if the disclosure is required by Law or Provider obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by Law or for the purpose for which it was disclosed to the person. Provider will further require that the person to whom information is disclosed inform the Provider of any breach of confidentiality or violation of the HIPAA Regulations with respect to that information. In such event, Provider will notify Plan of any instances of which it is aware in which the confidentiality of the information has been breached or the Privacy Rule was otherwise violated.

4.12. Reporting. Provider is not prohibited from using PHI to report violations of law to appropriate Federal and State authorities consistent with the Privacy Rule.

4.13. Access. The Plan acknowledges its obligation as a Covered Entity under the Privacy Rule to provide an Individual with access to that Individual's PHI in accordance with 45 C.F.R. 164.524. Pursuant to this BAA Agreement and with respect to Protected Health Information, Provider agrees to grant or deny requests for access, provide review of denials of access, when required under 45 C.F.R. § 164.524, and provide access to Individuals. In the event Provider uses or maintains an Electronic Health Record with respect to PHI of an Individual, Provider shall upon request provide an electronic copy of the PHI either to the Individual or directly to a third party designated by the Individual in accordance with the compliance date as provided in the HITECH Act and any guidance issued thereunder.

4.14. Mitigation. Provider agrees to mitigate, to the extent practicable, any harmful effect that is known to Provider resulting from a use or disclosure of PHI by Provider, or its Subcontractor, in violation of the requirements of this BAA Agreement or Applicable Law.

4.15. Plan Availability. Provider agrees to, within three (3) business days of receiving a request, make available to Plan or, at Plan's request, to Plan Sponsor, PHI that is relevant for Plan to carry out health plan functions under 45 C.F.R. § 164.504(f), provided the disclosures are subject to, and consistent with, the terms of the Provider Agreement.

4.16. Authorizations. With respect to PHI that Provider creates, receives, maintains, or transmits on behalf of Plan, Provider will be responsible for obtaining from an Individual any necessary authorizations to use or disclose that Individual's Protected Health Information, in accordance with 45 C.F.R. § 164.506 or 164.508; provided, however, that Plan Sponsor shall obtain any consent or authorization that may be required under applicable federal or state laws and regulations prior to Plan Sponsor's receipt of Private Health Information from Provider. Provider acknowledges that failure to obtain an authorization when necessary prior to disclosure constitutes a violation of this BAA Agreement and must be reported to Plan under section 4(c) of this BAA Agreement.

4.17. Restriction Requests. With respect to PHI that Provider creates, receives, maintains, or transmits on behalf of Plan, Provider will be responsible for receiving requests for restrictions from an Individual in accordance with 45 C.F.R. § 164.522 and for denying or agreeing to abide by any such requests. If Provider agrees to a restriction, Provider will be responsible for using and disclosing PHI consistent with that restriction. Failure to act in accordance with an agreed-to restriction constitutes a violation of this BAA Agreement and must be reported to Plan in accordance with section 4(c) of this BAA Agreement. If a request for restriction is made directly to Plan, Plan will refer such request to Provider for disposition in accordance with this subsection.

4.18. Confidential Communications. With respect to PHI that Provider creates, receives, maintains, or transmits on behalf of Plan, Provider will be responsible for receiving and acting upon requests for confidential communications from an Individual in accordance with 45 C.F.R. § 164.522. If Provider agrees to accommodate a request for confidential communications, Provider will be responsible for adhering to that accommodation. Failure to act in accordance with an accommodation that has been

granted constitutes a violation of this BAA Agreement and must be reported to Plan in accordance with section 4(c) of this BAA Agreement. If a request for confidential communications is made directly to Plan, Plan will refer Individual to Provider via customer service.

4.19. De-Identify. Provider may de-identify any and all PHI provided that Provider shall de-identify the information in accordance with HIPAA. De-identified information does not constitute Protected Health Information, and may be used by Provider or an affiliated entity for creating comparative databases, statistical analysis, or other studies.

4.20. Safeguards. Without limiting other provisions of this BAA Agreement, Provider agrees to (i) implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of EPHI that it creates, receives, maintains or transmits on behalf of Plan as required by the HIPAA Security Rule; and (ii) ensure that any Subcontractor to whom it provides EPHI agrees in writing to implement reasonable and appropriate safeguards to protect such information. Provider shall provide Plan with any such information concerning these safeguards as Plan may from time to time request.

4.21. Security Incidents. Provider agrees to promptly report to Plan any Security Incident of which it becomes aware.

5. **RESPONSIBILITIES OF PROVIDER REGARDING UNSECURED PHI**

5.1. Securing PHI. Unless it is not feasible under the circumstances, Business Associate agrees to implement, in a reasonable and appropriate manner, the technologies and methodologies the HITECH Act, the Secretary, or other Law specifies in order to render PHI that Provider creates, receives, maintains or transmits on behalf of Plan, unusable, unreadable, or indecipherable to unauthorized individuals, thereby making the PHI secure. In addition, unless it is not feasible under the circumstances, Provider shall ensure that any agent, including, but not limited to, Subcontractors or vendors to whom it provides Plan's PHI will implement, in a reasonable and appropriate manner, the technologies and methodologies the HITECH Act, the Secretary, or other Law specifies with respect to rendering Plan's PHI unusable, unreadable or indecipherable to unauthorized individuals.

5.2. Breach Notification. With respect to any Unsecured PHI, Provider shall report to Plan any Breach (as defined in the Omnibus Rule) discovered by Provider, or any of Provider's Subcontractors, within twenty-four (24) hours of Discovery.

(a) The report must include (or be supplemented on an ongoing basis as information becomes available) with: (i) the identification of all Individuals whose Unsecured PHI was or is believed to have been breached; (ii) a brief description of the Breach, including the type of Breach (e.g, theft, loss, improper disposal, hacking), location of the Breach (e.g., laptop, desktop, paper), how the Breach occurred, the date the Breach occurred, and the date the Breach was discovered; (iii) a description of the type of Unsecured PHI involved (e.g., social security number, diagnosis, EOBs, etc.), including the type of media, but not the Breached PHI itself, unless requested by Plan; (iv) a description of the safeguards in place prior to the Breach (e.g., firewalls, packet filtering, secure browser sessions, strong authentication); (v) a description of the actions taken in response to the Breach (e.g., additional safeguards, mitigation, sanctions, policies, and procedures); (vi) all other information reasonably requested by Plan to enable Plan to perform and document a risk assessment in accordance with the Breach Notification Rule, and (vii) all other information reasonably necessary to provide notice to Individuals, the Secretary and/or the media.

(b) At Plan's sole option, Plan may delegate to Provider the responsibility for determining (and providing evidence to Plan) that any such incident is not a Breach, including the requirement to perform a risk assessment to determine whether a low probability of compromise has occurred, as provided by the Breach Notification Rule. In the event that Plan delegates this obligation to Provider, without unreasonable delay, and in any event no later than thirty (30) calendar days after Discovery, Provider shall provide Plan with written notification of the Breach and a copy of the risk assessment that assesses whether a low probability of compromise occurred.

(c) At Plan's sole option, Plan may delegate to Provider the responsibility of providing any notifications Plan determines is required by the Breach Notification Rule, including notifications to Individuals, the Secretary and/or the media. Prior to sending out such notifications, Provider will provide a copy of the template notification letters for approval by Plan. All notifications shall comply with the elements established by the Breach Notification Rule and be sent within timeframes established by the Breach Notification Rule. In the event that Plan delegates these obligations to Provider and in the event of a Breach, without unreasonable delay, and in any event no later than sixty (60) calendar days after Discovery, Provider shall provide Plan evidence that all required notifications, including any media or Secretary notifications, have been made.

(d) Provider shall pay all reasonable costs incurred in relation to the occurrence of a Breach or potential Breach, including, but not limited to, expenses relating to providing any notifications Plan, or as applicable the Provider, determines necessary under the Breach Notification Rule, regardless of whether Provider or Plan makes the notifications.

6. **RESPONSIBILITIES OF PLAN.** Plan agrees to amend Plan documents to include specific provisions to restrict the use or disclosure of PHI and to ensure adequate procedural safeguards and accounting mechanisms for such uses or disclosures, in accordance with the Privacy Rule.

7. **TERM AND TERMINATION.**

7.1. Term. The term of this BAA Agreement shall continue until termination of the Provider Agreement or until otherwise terminated pursuant to this BAA Agreement.

7.2. Termination and Amendment by Operation of Law. This BAA Agreement shall terminate immediately in the event that a HIPAA Business Associate Agreement is no longer applicable or required under then current Law. If on the advice of Plan's counsel, Plan reasonably determines that the terms of this BAA Agreement likely would be interpreted to violate or not comply with any Applicable Laws, the parties shall negotiate in good faith to amend this BAA Agreement to comply with such Laws. If the parties cannot reasonably agree on such amendment, then this BAA Agreement and the Provider Agreement, if one, shall terminate.

7.3. Termination by Plan. Plan may terminate this BAA Agreement if it reasonably determines that Provider has violated a material term of this BAA Agreement, the HIPAA Regulations, or any other Applicable Law after providing thirty (30) days for Provider to cure the breach in cooperation with Plan or end the violation; provided, however, that in the event that termination of this BAA Agreement is not feasible in Plan's sole discretion, Provider hereby acknowledges that Plan shall have the right to immediately terminate this BAA Agreement and the Provider Agreement, if any, and to report the breach to the Secretary, notwithstanding any other provision of this BAA Agreement to the contrary.

7.4. Right to Cure. In the event that Provider breaches this BAA Agreement or any provision of the Privacy Rule and fails to cure the breach within thirty (30) days, Plan reserves the right to cure such breach. Provider will cooperate with any such efforts undertaken by Plan. Cure of breach does not limit Plan's ability to immediately terminate this BAA Agreement and the Provider Agreement, if any.

7.5. Injunctive Relief. Provider acknowledges and agrees that the terms of this BAA Agreement and the HIPAA Regulations are necessarily of a special, unique and extraordinary nature and that the loss arising from a breach thereof cannot reasonably and adequately be compensated by money damage, as such breach will cause Plan to suffer irreparable harm. Accordingly, upon failure of Provider to comply with the terms of the Provider Agreement, HIPAA Regulations, or other Applicable Law, and except as otherwise provided herein, Plan or any of its successors or assigns shall be entitled to injunctive or other extraordinary relief and with such injunctive or other extraordinary relief to be cumulative to, but not in limitation of, any other remedies that may be available to Plan, its successors or assigns, such relief to be without the necessity of posting a bond.

7.6. Effect of Termination. Upon termination or expiration of this BAA Agreement, Provider shall either return or destroy all PHI created, received, maintained, or transmitted by Provider on behalf of Plan that the Provider maintains in any form and shall retain no copies of such information to the extent that such action is feasible and not prohibited by other Applicable Law. This provision applies to all Subcontractors or agents of Provider who may possess PHI on behalf of the Provider and/or Plan. In the event that Plan has ascertained that the return or destruction of such information is not feasible or permissible, Provider agrees to continue to comply with all provisions of this BAA Agreement with regard to its uses, storage, and disclosure of such PHI for as long as Provider maintains such PHI.

7.7. General Permitted Uses and Disclosures**.** Except as otherwise limited in this BAA Agreement, Provider may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Plan as specified in the Provider Agreement, provided that such use or disclosure would not violate the HIPAA Regulations or other Law if performed by Plan itself.

8. **INDEMNIFICATION.** Each party shall indemnify and defend the other party against and hold it harmless from all claims, damages, losses, judgments, costs and expenses (including attorneys' fees) arising out of the indemnifying party's negligence or intentional misconduct in such party's use, disclosure or storage of PHI and/or such party's breach of this BAA Agreement.