APEX Partner Data Processing Addendum

This APEX Partner Data Processing Addendum ("**Partner DPA**") to the Agreement shall apply where the parties to the Agreement may exchange Personal Data in the performance of their obligations, including provision of services (the "**Services**") by Dell, under the Agreement. In the event of conflict between this Partner DPA and the Agreement, this Partner DPA shall control with respect to its subject matter.

1. Definitions.

Terms not defined herein have the meanings set forth in the Agreement. The following words in this Partner DPA have the following meanings:

1.1 "Agreement" means the Dell APEX Reseller Agreement, Dell APEX Distributor Agreement, or any substantially similar agreement under which Dell provides the Service.

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 "GDPR" means the General Data Protection Regulation (EU) 2016/679.

1.4 "Model Clauses" means, as applicable:

(i) 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 third countries;

(ii) the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for international data transfers or the International Data Transfer Agreement, each as issued under § 119A of the Data Protection Act 2018 in respect of transfers from the United Kingdom ("**UK**") to countries which are not subject to an adequacy decision under the UK GDPR; or

(iii) 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 and as specifically amended for use under the Swiss Federal Data Protection Act by the amendments announced by the Swiss Federal Data Protection and Information Commissioner on 27 August 2021, in respect of transfers from Switzerland to third countries.

1.5 "Personal Data" means any information relating to an identified or identifiable natural person, or as otherwise defined as "personal data" or "personal information" under the Privacy Laws, which is Processed by the parties in the performance of the Agreement.

1.6 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data Processed under this Partner DPA.

1.7 "Privacy Laws" means any data protection and privacy laws to which a party to the Agreement is subject and which are applicable to the Services provided, including where applicable, the GDPR, UK GDPR, the California Consumer Privacy Act ("CCPA") and other similar laws.

1.8 "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9 "Processor" means an entity which Processes the Personal Data on behalf of the Controller.

1.10 "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 Disclosing Controller to Receiving Controller for the purposes of performing the parties' obligations under the Agreement.

1.11 "Subprocessor" means a third party engaged by either party, acting as a Processor, (including without limitation

an affiliate and/or subcontractor) in connection with the Processing of the Personal Data by either party pursuant to this Partner DPA.

1.12 "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.

2. Compliance

The parties agree to comply with their respective obligations under any relevant Privacy Laws that apply to the relationship contemplated under the Agreement and to Process any Personal Data only in compliance with applicable Privacy Laws. Each party has responsibility for complying with Privacy Laws regarding the lawfulness of the Processing of Personal Data prior to disclosing, transferring, or otherwise making available, any Personal Data to the other party and shall have obtained all rights and authorizations necessary to disclose the Personal Data to the other party, including but not limited to giving the appropriate notices and, where necessary, obtaining consents from the Data Subject (in accordance with Privacy Laws) to the disclosure of their Personal Data in connection with the Agreement.

3. Controller to Controller

Where one party acting as a Controller ("Disclosing Controller") discloses Personal Data to the other party to also Process as a Controller ("Receiving Controller") the following obligations will apply:

3.1 unless the parties otherwise agree in writing, Receiving Controller will Process the Personal Data solely for the purpose of performing its obligations under the Agreement and in accordance with applicable Privacy Laws. The Receiving Controller shall not Process the Personal Data for any activity or purpose unless expressly permitted by Privacy Laws;

3.2 Personal Data is provided to the Receiving Controller solely for the purpose of performing its obligations under the Agreement. Disclosing Controller does not provide any monetary or other non-monetary valuable consideration for access to or other processing of Personal Data except for payments agreed under the Agreement for the performance of the Services under the Agreement;

3.3 If Disclosing Controller discloses Personal Data for the purpose of Receiving Controller sending marketing communications, Disclosing Controller agrees to obtain the relevant Data Subjects' prior consent to such disclosure and use by Receiving Controller;

3.4 Each Party shall comply promptly with its obligations to respond to requests from data subjects to exercise their rights under Privacy Laws (including their rights to withdraw consent, of access, restriction, rectification, erasure and portability) in respect of the Personal Data. Receiving Controller will deal promptly with all reasonable inquiries from Disclosing Controller or a Data Subject relating to the Personal Data, including requests for access or correction of Personal Data and information about Receiving Controller's practices, procedures and/or complaints process;

3.5 In the event a party receives a request or notification from a third party (including a data protection supervisory authority) or an order of court that concerns the Personal Data processed under the Agreement, it shall promptly notify the other Party, providing all relevant details. The Parties shall reasonably cooperate with each other to respond to such request or notification. Unless required by law, neither Party shall respond to any request or notification on behalf of the other Party unless instructed to do so in writing by such other Party;

3.6 If a Personal Data Breach occurs in connection with the Agreement, the Party experiencing the Personal Data Breach shall notify the other Party without undue delay after becoming aware. Each Party shall cooperate with and assist the other in handling, mitigating and/or resolving a Personal Data Breach. The Parties shall, following consultation with each other, comply with any applicable obligations under Privacy Laws to notify the relevant supervisory authorities and/or data subjects;

3.7 The Receiving Controller shall erase and/or destroy the Personal Data after termination of the Agreement if it is no longer necessary to retain it for the purpose of the Agreement or as otherwise required by applicable laws;

3.8 Receiving Controller is prohibited from: (i) Selling any Personal Data; (ii) retaining, using, or disclosing Personal Data for any purpose other than for the specific purpose of performing the obligations under the Agreement, including but not limited to, retaining, using, or disclosing Personal Data for a commercial purpose other than fulfilling the Agreement; and (iii) retaining, using, or disclosing Personal Data outside of the direct business relationship between Disclosing Controller and Receiving Controller; and

3.9 Receiving Controller represents and warrants that it understands the prohibitions and limitations regarding its use and all other processing activities and related purposes as outlined in this Partner DPA regarding Personal Data, particularly in Section 3.8 and will comply with them.

4. Controller to Processor

Where one party acting as a Controller discloses Personal data to the other party to Process as a Processor or Subprocessor on its behalf, the party acting as a Processor or Subprocessor shall:

4.1 Process the Personal Data only in accordance with the Controller's instructions, unless required to do so by applicable law. Any additional or alternate Processing instructions not contained in this Partner DPA must be agreed between the parties in writing, including the costs (if any) associated with complying with such instructions. Neither party is responsible for determining if the Controller's instructions are compliant with applicable law. However, if either party is of the opinion that a Controller instruction infringes applicable Privacy Laws, that party shall notify the other as soon as reasonably practicable and shall not be required to comply with such infringing instruction. Details of the subject matter of the Processing, its duration, nature and purpose, and the type of Personal Data and data subjects are as specified in the Agreement and Annex 2;

4.2 Process the Personal Data provided by the Controller only to the extent necessary to perform its obligations under the Agreement;

4.3 Not disclose the Personal Data to any third party (other than an affiliate or Subprocessor) except as necessary and only for the purposes of:

(a) complying with the Controller's instructions;

(b) complying with this Partner DPA; or

(c) complying with the law or a binding order of a governmental body. Unless it would violate the law or a binding order of a governmental body, Processor will give the Controller notice of any legal requirement or order referenced in this provision;

4.4 Upon becoming aware of a Personal Data Breach, (i) notify the Controller without undue delay (and in any event within 72 hours); (ii) provide written details of the Personal Data Breach to the extent such information is known or available to the Processor at the time; (iii) use reasonable efforts to assist the other party in mitigating, where possible, the adverse effects of any Personal Data Breach; and (iv) implement all measures required by Privacy Laws in case of such Personal Data Breach;

4.5 Upon reasonable prior written request, provide the Controller with such information as may be reasonably necessary under applicable law to demonstrate Processor's compliance with this Partner DPA;

4.6 Upon reasonable prior notice, provide reasonably requested assistance to the Controller to carry out data protection impact assessments and/or prior consultations to the extent required by Privacy Laws in relation to the Processing of Personal Data by that party as a Processor;

4.7 Promptly notify Controller of, and cooperate with the Controller to address, any requests from individuals or applicable data protection authorities relating to the Processing of Personal Data under the Agreement, including requests from individuals seeking to exercise their rights under any applicable Privacy Laws. Processor shall not respond to such communications directly without Controller' prior authorization, unless legally compelled to do so;

4.8 At the expiry or termination of the Agreement, or otherwise at Controller's option (as may be requested in writing), delete or return all Personal Data to Controller as soon as reasonably practicable, except where the Processor is required to retain copies under applicable law, in which case Processor will limit and protect that Personal Data from any further Processing except to the extent required by applicable law;

4.9 If either party is Processing Personal Data within the scope of the CCPA, that party shall Process Personal Data on behalf of the other party only and will not retain, use, share or disclose that Personal Data for any purpose other than for the purposes set out in this Partner DPA, the Agreement and as permitted under the CCPA or any subsequent law. In no event will either party share any Personal Data with third parties (except to Subprocessors in accordance with clause 5 below) or sell any Personal Data. Each party certifies that it understands and will comply with all restrictions placed on its Processing of Personal Data, including by avoiding any action that would cause the other party to be deemed to have sold Personal Data or Personal Information under the CCPA. For purposes of this paragraph, Processors hereunder will be considered Service Providers as defined in Section 1798.140(v) of the CCPA;

and

4.10 Upon reasonable prior written request from the other party (such request to be made in accordance with the terms of the Agreement), provide such information as may be reasonably necessary to demonstrate compliance with the Processor's obligations under this Partner DPA and allow for and contribute to audits, including inspections, conducted by the other party or another auditor mandated by that party.

5. Subprocessors.

5.1 Use of Subprocessors.

Either party may and has general consent from the other party to use Subprocessors, Parties may appoint and use Subprocessors to process the Personal Data in connection with the Services under the Agreement provided that, in each case, it has in place a contract in writing with each Subprocessor that is relevant to the services to be provided by the Subprocessors and under which the Subprocessor (i) provides sufficient guarantees to implement appropriate technical and organisational measures and (ii) abides by terms materially similar to the rights and/or obligations imposed on Dell under this Partner DPA. Subprocessors may include third parties or any affiliate of a party. Where a Subprocessor fails to fulfil its data protection obligations as specified above, the relevant Processor having engaged that Subprocessor shall be liable to the other party for the performance of the Subprocessors' obligations.

5.2 List of Subprocessors.

A list of Subprocessors that Dell engages to support the provision of its' services is made available by Dell on www.dell.com/subprocessors.

6. Security.

6.1 Technical and organisational security measures.

Each party will ensure that it has appropriate technical and organisational measures in place to reasonably ensure that the security, confidentiality, integrity, availability and resilience of Processing systems and services involved in the Processing of any Personal Data are commensurate with the risk in respect of such Personal Data and to guard against a Personal Data Breach. The Parties agree that the technical and organisational security measures described in Annex 1 ("**Information Security Measures**") provide an appropriate level of security for the protection of Personal Data to meet the requirements of this Partner DPA. Each party will periodically (i) test and monitor the effectiveness of its safeguards, controls, systems and procedures and (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Data, and ensure these risks are addressed.

6.2 Technical Progress

The Information Security Measures are subject to technical progress and development and Dell may modify these provided that such modifications do not degrade the overall security of the Personal Data processed under the Agreement.

6.3 Access.

The parties shall ensure that persons authorized to access the Personal Data (including any affiliate or authorized Subprocessor) are under a duty of confidence and will respect and maintain the confidentiality and security of the Personal Data and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. International Transfers.

The parties are authorized, in connection with the Processing of Personal Data under this Partner DPA, or in the normal course of business, to make worldwide transfers of Personal Data to their respective affiliates and/or Subprocessors. When making such transfers, each party shall ensure appropriate protection is in place to safeguard the Personal Data transferred under or in connection with this Agreement. Where the fulfilment of the parties' obligations under the Agreement involves the transfer of Personal Data from the European Economic Area ("EEA") or the UK or Switzerland to countries outside the EEA or the UK or Switzerland (which are not subject to an adequacy decision under Privacy Laws) the parties agree that they will use the Model Clauses along with appropriate supplemental measures or other appropriate data transfer mechanisms in accordance with applicable Privacy Laws and, in particular, such transfers shall be subject to: (a) each party having in place intra-group agreements with its'

Affiliates which may have access to the Personal Data, which agreements shall incorporate the relevant Model Clauses and (b) each party having in place agreements with its' Subprocessors that incorporate the relevant Model Clauses as appropriate. Where the fulfilment of the parties' obligations under the Agreement involves the transfer of Personal Data across other international borders requiring one or more additional Personal Data transfer compliance mechanisms under applicable Privacy Laws, the parties agree that they will use the appropriate contractual clauses or other prescribed mechanism(s) and/or measure(s) to ensure the compliant transfer of Personal Data across those borders, as required under the Privacy Laws and/or promulgated by the relevant data privacy regulator.

8. Survival.

Each Party's obligations under this Partner DPA shall survive the termination of the Partner DPA and the Agreement and continue in effect for as long as the Personal Data continues to be in the Receiving Controller's possession or control.

Annex 1

Information Security Measures

Dell takes information security seriously. This information security overview applies to Dell's corporate controls for safeguarding personal data which is processed and transferred amongst Dell group companies. Dell's information security program enables the workforce to understand their responsibilities. Some customer solutions may have alternate safeguards outlined in the statement of work as agreed with each customer.

Security Practices

Dell has implemented corporate information security practices and standards that are designed to safeguard the Dell's corporate environment and to address: (1) information security; (2) system and asset management; (3) development; and (4) governance. These practices and standards are approved by the Dell CIO and undergo a formal review on an annual basis.

Organizational Security

It is the responsibility of the individuals across the organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, the function of information security provides:

1. Strategy and compliance with policies/standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and drives the security direction of the company.
2. Security testing, design and implementation of security solutions to enable security controls adoption across the environment.
3. Security operations of implemented security solutions, the environment and assets, and manage incident response.
4. Forensic investigations with security operations, legal, data protection and human resources for investigations including eDiscovery and eForensics.

Asset Classification and Control

Dell's practice is to track and manage physical and logical assets. Examples of the assets that Dell IT 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 may include controls such as access management, encryption, logging and monitoring, and data destruction.

Personnel Security

As part of the employment process, employees undergo a screening process applicable per regional law. Dell's annual compliance training includes a requirement for employees to complete an online course and pass an assessment covering information security and data privacy. The security awareness program may also provide materials specific to certain job functions.

Physical and Environmental Security

Dell uses a number of technological and operational approaches in its physical security program in regards to risk mitigation. The security team works closely with each site to determine appropriate measures are in place and continually monitor any changes to the physical infrastructure, business, and known threats. It also monitors best practice measures used by others in the industry and carefully selects approaches that meet both uniqueness's in business practice and expectations of Dell as a whole. Dell balances its approach towards security by considering elements of control that include architecture, operations, and systems.

Communications and Operations 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.

Incident response procedures exist for security and data protection incidents, which may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

To protect against malicious use of assets and malicious software, additional controls may be implemented, based on risk. Such controls may include, but are not limited to, information security practices and standards; restricted access; designated development and test environments; virus detection on servers, desktops and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; 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.

Access Controls

Access to corporate systems is restricted, based on procedures to ensure appropriate approvals. To reduce the risk of misuse, intentional or otherwise, access is provided based on segregation of duties and least privileges.

Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place.

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

System Development and Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in the Dell environment. Based on risk to Dell'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 applicable to Dell corporate. These requirements cover areas such as intellectual property of the company and our 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 2
Data Processing Description

1. Subject matter and duration of the Processing.

The subject matter and duration of the Processing shall be according to the Agreement.

2. Purpose of Processing.

Personal Data will be Processed for the purpose of performing obligations under the Agreement.

3. Nature of Processing.

Personal Data will be Processed as required to meet the parties' obligations under the Agreement.

4. Categories of Data Subjects.

The data subjects are parties' end users, employees, contractors, suppliers and other third parties relevant to the relationship of the parties under the Agreement.

5. Types of Personal Data.

The type of personal data that may be submitted are:

- Contact details: which may include name, address, email address, telephone, and other contact information.
- End customer details: which may include contact details, invoicing and credit related data.
- IT systems and operational information: which may include personal identifiers, voice, video and data recordings, user ID and password details, computer name, email address, domain name, user names, passwords, IP address, permission data (according to job roles), account and delegate information for communication services, individual mailboxes and directories, chat communication data, software and hardware inventory, tracking information regarding patterns of software and internet usage (e.g. cookies), and information recorded for operational and/or training purposes).
- Data subjects' email content and traffic/transmission data; online interactive and voice communications (such as blogs, chat, webcam and networking sessions); support services (incidental access may include accessing the content of email communications and data relating to the sending, routing and delivery of emails).
- Other: Any other Personal Data submitted by one party to the other.