Dell EMC Customer Standard Data Protection Schedule

This Data Protection Schedule ("**Schedule**") shall apply where the provision of relevant Services by Dell to you / Customer ("**Customer**") involves the processing of Personal Data (as defined below) which is subject to Privacy Laws (as defined below). In the event of conflict between this Schedule and the relevant Customer Agreement (meaning the 'Agreement' based on Dell EMC's Commercial Terms of Sale or other negotiated sales agreement referring to this Schedule), this Schedule shall control with respect to its subject matter.

1. **Definitions**: The following words have the following meanings:

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

   (b) "**Model Clauses**" means the Standard Contractual Clauses (Controller to Processor) approved by the EU Commission for transfers of personal data to countries outside the European Economic Area ("EEA") that have not been deemed by the European Commission as providing an adequate level of data protection.

   (c) "**Personal Data**" means any information relating to an identified or identifiable natural person which is processed by Dell, acting as a Processor on behalf of the Customer, in connection with the provision of the Services and which is subject to Privacy Laws.

   (d) "**Privacy Laws**" means any data protection and/or privacy related laws, statutes, directives, or regulations (and any amendments or successors thereto) to which a party to the relevant Customer Agreement is subject and which are applicable to the Services provided.

   (e) "**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.

   (f) "**Processor**" means an entity which processes the Personal Data on behalf of the Controller.

   (g) "**Security Incident**" means a material breach by Dell of the security obligations under this Schedule leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored or otherwise processed.

   (h) "**Subprocessor**" means a third party engaged by Dell (including without limitation a Dell affiliate and/or subcontractor of Dell) in connection with the processing of the Personal Data in relation to the provision of the Services.

2. **Instructions and details of processing**: Customer authorizes Dell to process the Personal Data to provide the Services in accordance with Dell's rights and obligations under the relevant Customer Agreement and in any subsequent statements of work or service orders, and to use performance data derived from the provision of the Services and the processing of the Personal Data to enhance and/or improve Dell's products and services. This Schedule, the relevant Customer Agreement and any subsequent statements of work or services orders, comprise Customer's complete instructions to Dell regarding the processing of Personal Data. Any additional or alternate instructions must be agreed between the parties in writing, including the costs (if any) associated with complying with such instructions. Customer agrees that it will not require Dell to undertake or engage in any activity that would require, or result in, Dell acting in the capacity of a Controller. Dell is not responsible for determining if Customer's instructions are compliant with applicable law. However, if Dell is of the opinion that a Customer instruction infringes applicable Privacy Laws, Dell shall notify Customer 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 description of the Services, the relevant Customer Agreement and/or appendix 1 of the Model Clauses (if executed). Except as otherwise expressly stated, Customer is the Controller and Dell is the Processor of the Personal Data processed under the Customer Agreement.

3. **Disclosures**: Dell may only disclose the Personal Data to third parties (including its Subprocessors, Dell affiliates and subcontractors) for the purpose of: (a) complying with Customer's reasonable and lawful instructions; (b) as required in connection with the Services and as permitted by this Schedule and/or (c) as required to comply with Privacy Laws, or an order of any court, tribunal, regulator or government agency with competent jurisdiction to which Dell is subject PROVIDED that Dell will (to the extent permitted by law) inform the Customer in advance of making any disclosure of Personal Data and will reasonably co-operate with Customer to limit the scope of such disclosure to what is legally required.

4. **Compliance with laws**: Customer and Dell agree to comply with their respective obligations under Privacy Laws applicable to the Services. Customer warrants and represents (on its behalf and on behalf of each of its affiliates) that it has obtained all necessary authorisations and consents required for compliance with Privacy Laws prior to disclosing, transferring, or otherwise making available, any Personal Data to Dell. Dell shall, as required in connection with the Services and to the extent commercially practicable, assist Customer to respond to requests for exercising the rights of individuals under applicable Privacy Laws. Dell reserves the right to charge Customer for such assistance if the cost of assisting exceeds a nominal amount. Dell shall notify Customer as soon as reasonably practicable of any request Dell receives from individuals relating to the exercise of their rights under applicable Privacy Laws during the term of the relevant Customer Agreement (to the extent such request relates to the Personal Data).

5. **Confidentiality**: To the extent the Personal Data is confidential (pursuant to applicable law), Dell shall maintain the confidentiality of the Personal Data and shall ensure that Dell employees or representatives authorized to process the Personal Data (including its Subprocessors) have committed themselves to obligations of confidentiality.

6. **Security**: Taking into account industry standards, the costs of implementation, the nature, scope, context and purposes of the processing and any other relevant circumstances relating to the processing of the Personal Data, Dell shall implement appropriate technical and organisational measures to ensure security, confidentiality, integrity, availability and resilience of processing systems and services involved in the processing of the Personal Data are commensurate with the risk in respect of such Personal Data. The parties agree that the 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 clause. Dell 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. Dell shall have implemented and documented appropriate business continuity and disaster

recovery plans to enable it to continue or resume providing Services (including restoring access to the Personal Data where applicable) in a timely manner after a disruptive event. Dell will periodically test and monitor the effectiveness of its business continuity and disaster recovery plans. Dell will provide a summary of its written business continuity and disaster recovery plans to Customer upon written request.

7. **International Transfers**: Dell is authorised, in connection with the provision of the Services, or in the normal course of business, to make worldwide transfers of Personal Data to its affiliates and/or Subprocessors. When making such transfers, Dell shall ensure appropriate protection is in place to safeguard the Personal Data transferred under or in connection with the relevant Customer Agreement. Where the provision of Services involves the transfer of Personal Data from the EEA to countries outside the EEA (which are not subject to an adequacy decision under Privacy Laws) such transfer shall be subject to the following requirements: (a) Dell has in place intra-group agreements with any Dell affiliates which may have access to the Personal Data, which agreements shall incorporate the Model Clauses; and (b) Dell has in place agreements with its Subprocessors that incorporate the Model Clauses as appropriate.

8. **Subprocessors**: Customer agrees that Dell may appoint and use Subprocessors to process the Personal Data in connection with the Services PROVIDED that: (a) Dell puts in place a contract in writing with each Subprocessor that imposes obligations that are (i) relevant to the services to be provided by the Subprocessors and (ii) materially similar to the rights and/or obligations granted or imposed on Dell under this Schedule; and (b) where a Subprocessor fails to fulfil its data protection obligations as specified above, Dell shall be liable to the Customer for the performance of the Subprocessor's obligations.

9. **Privacy Impact Assessment (PIA) clause**: Dell shall provide reasonable cooperation and assistance to Customer, to the extent applicable in relation to Dell's processing of the Personal Data and within the scope of the agreed Services, in connection with any data protection impact assessment(s) which the Customer may carry out in relation to the processing of Personal Data to be undertaken by Dell, including any required prior consultation(s) with supervisory authorities. Dell reserves the right to charge Customer a reasonable fee for the provision of such cooperation and assistance.

10. **Security Incidents:** Where a Security Incident is caused by Dell's failure to comply with its obligations under this Schedule, Dell shall where required by applicable Privacy Laws, notify Customer without undue delay after establishing the occurrence of the Security Incident and shall:

    (a) to the extent such information is known or available to Dell at the time, provide Customer with details of the Security Incident, a point of contact, and the measures taken or to be taken to address the Security Incident;

    (b) reasonably cooperate and assist Customer with any investigation into, and/or remediation of, the Security Incident (including, without limitation and where required by Privacy Laws, the provision of notices to regulators and affected individuals);

    (c) not inform any unaffiliated third party (other than a Subprocessor potentially possessing relevant information, or experts or consultants utilized by Dell) of any Security Incident relating to the Personal Data without first obtaining Customer's prior written consent, except as otherwise required by applicable law. Nothing in this clause shall prevent Dell from notifying other customers whose personal data may be affected by the Security Incident;

    (d) in the event Customer intends to issue a notification regarding the Security Incident to a data protection supervisory authority, other regulator or law enforcement agency, Customer shall (unless prohibited by law) allow Dell to review the notification and Customer shall have proper consideration to any reasonable comments or amendments proposed by Dell.

11. **Deletion of Personal Data:** Upon termination of the Services (for any reason) and if requested by Customer in writing, Dell shall, as soon as reasonably practicable and in accordance with applicable law, delete the Personal Data, PROVIDED that Dell may: (a) retain one copy of the Personal Data as necessary to comply with any legal, regulatory, judicial, audit or internal compliance requirements; and (b) defer the deletion of the Personal Data to the extent and for the duration that any Personal Data or copies thereof cannot reasonably and practically be expunged from Dell's systems. For such retention or deferral periods as set out in subparagraphs (a) and (b) of this clause, the provisions of this Schedule shall continue to apply to such Personal Data. Dell reserves the right to charge Customer for any reasonable costs and expenses incurred by Dell in deleting the Personal Data pursuant to this clause.

12. **Demonstrating Compliance:** Dell shall, upon reasonable prior written request from Customer (such request not to be made more frequently than once in any twelve-month period), provide to Customer such information as may be reasonably necessary under applicable law to demonstrate Dell's compliance with its obligations under this Schedule.

13. **Liability and Costs**: Neither Dell nor any Subprocessor shall be liable for any claim brought by Customer or any third party arising from any action or omission by Dell and/or Subprocessors to the extent such action or omission resulted from compliance with Customer's instructions (including Customer's security practices, policies and/or processes).

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 align to uniqueness in business practices 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.