Data Processing Addendum

The terms of this Data Processing Addendum ("**DPA**") are incorporated by reference to the Master Agreement between you and Blackboard ("we", "us" and "our") (the "**Agreement**").

The following provisions shall apply whenever Personal Information is Processed under the Agreement:

1. Definitions

Capitalized terms not defined in this section have the meaning given in the Agreement.

Applicable Data Privacy Laws means laws and regulations that apply to our and your Processing of Personal Information under this Agreement. In the United States, this may include the Family Education Rights Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children's Online Privacy Protection Act (COPPA), as well as applicable State student and consumer privacy laws (such as the California Consumer Privacy Act (CCPA), once in effect). In the European Union (and outside the EU, if extraterritorially applicable), this will include General Data Protection Regulation ("GDPR") and the national laws implementing GDPR, as applicable. In Australia, this may include the Privacy Act 1998 and amendments. In South Africa, this may include the Protection of Personal Information Act of 2013 (POPIA) once effective.

De-Identified Data means information that has all identifying Personal Information obscured or removed such that the remaining information does not reasonably identify an individual nor allow a reasonable person to identify an individual with reasonable certainty.

Individual Right Request means a request from your Authorized End Users or other individuals concerning the exercise of their rights available under Applicable Data Privacy Law in relation to Personal Information, including the right of access, right to correct, right to restrict Processing, right to erasure ("right to be forgotten"), right to data portability, right to object to the Processing and right not to be subject to an automated individual decision making.

Personal Information means information Processed by Blackboard on your behalf in connection with the provision of Products and Services pursuant to the Agreement that relates to, describes or is linked to an identified or identifiable individual. For clarity and without limitation, Personal Information may include: (i) in the United States, personal information that is contained in "educational records" as defined by the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232(g); and (ii) "personal information" or "personal data" as such terms are defined by the Applicable Data Privacy Laws in your jurisdiction.

Processing means any operation or set of operations which is performed on Personal Information 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. For the avoidance of doubt Processing shall include all means, operations and activities performed on Personal Information that are defined as processing under GDPR.

Security Incident means a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information.

Service Providers (Sub-processors) means Blackboard affiliates and subsidiaries or third party vendors which we engage in connection with the Agreement and which Process Personal Information on behalf of us and under our instructions.

2. **Roles and responsibilities of the parties**

2.1 You are the controller of Personal Information. We are the processor (as defined in the GDPR) or service provider (as defined under CCPA) and Process Personal Information on your behalf and subject to your instructions. Unless otherwise expressly indicated, if you are subject to regulations in the United States, we Process Personal Information relating to students as a School Official performing an outsourced institutional function, pursuant to FERPA 34 CFR Part 99.31(a)(1). When we Process Personal Information on your behalf, you retain all right, title and interest to such Personal Information and Blackboard does not own, control, or license such information except as described in the Agreement.

2.2 To the extent the GDPR applies to the Personal Information, the subject matter and a description of scope and purpose of the processing of Personal Information, including the type of Personal Information and categories of data subjects, are set out in the Agreement and Annex A of this DPA. We and you have entered into the Agreement to benefit from our expertise in Processing Personal Information solely for the purposes set out herein and in the Agreement. We shall be allowed to exercise our own discretion in the selection and use of means as we consider necessary to pursue those purposes, subject to the requirements of this DPA and Applicable Data Privacy Laws.

3. **Blackboard's obligations**

3.1 Blackboard (together with its employees, affiliates, and subsidiaries), may Process the Personal Information as a service provider and, in doing so, may retain, use, disclose and otherwise Process Personal Information solely in accordance with your written instructions and for the following purposes: (i) providing Products and Services to you including any functionalities activated by your system administrators, (ii) maintaining and supporting our Products and Services; (iii) as otherwise permitted or required by applicable Law.

3.2 The Agreement and the DPA are your written instructions to us in relation to the processing of Personal Information. We agree to follow such instructions with regard to the Processing of Personal Information. Our obligations under Sections 3.1 and this 3.2 shall be subject to Section 4.2.

3.3 Provided that we Process only the minimum amount of Personal Information necessary, and the output of the Processing is aggregated or De-identified Data (to which we implement appropriate technical safeguards and businesses processes to prevent the re-identification of individuals), you agree that we may Process Personal Information for additional lawful purposes, including: (i) evaluating, improving and/or developing our Products and Services; (ii) developing new Products and Services; and (iii) analytics and research. We may also Process Personal Information as necessary to enforce our rights under the Agreement. We may suggest supplemental educational tools or services to Authorized Users to the extent consistent with applicable Law; however, we will not use Personal Information for targeted advertising, without the consent of you or your Authorized Users.

3.4 You acknowledge that where we process personal information: (i) in the context of a direct relationship we have with an Authorized User in the course of providing or offering services to them; or (ii) with the consent of an Authorized User solely with respect to their own personal information, our Processing activities are outside the scope of this DPA. You agree to Blackboard's fulfilment of any legally satisfactory request and consent by an Authorized User to download, export, save, maintain or transfer their own personal information.

3.5 In the unlikely event that applicable law requires us to Process Personal Information other than as instructed, we will notify you unless prohibited from so doing by applicable Law.

3.6 We agree to uphold our responsibilities under Applicable Data Privacy Laws and to supervise and train our employees accordingly. We will ensure that such persons with access to Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.7 We will promptly notify you about any legally binding request for disclosure of Personal Information by a law enforcement authority or other organization or body, unless legally prohibited. Where legally permissible, we will refer the requesting authority to you and will otherwise provide you with reasonable assistance in relation to such requests. This will include (i) ensuring that the request is legally binding and valid, (ii) conducting a legal assessment of the extent to which we are required by law to comply with the request and the requirements under Applicable Data Privacy Laws that may restrict such disclosure, and (iii) not providing more Personal Information than strictly necessary to comply with the request.

4. **Your obligations**

4.1 You warrant your collection and sharing of Personal Information with us shall comply with Applicable Data Privacy Laws.

4.2 You warrant that you will give only lawful instructions. If we hold the view that any instruction of yours contravenes applicable law and/or the DPA, we will notify you, and we are entitled to suspend execution of the instruction, until you confirm such instruction in writing. We have the right to deny the execution of an instruction – even if issued in writing – in case we conclude that we would be liable under applicable law if we execute the instructions you have provided.

4.3 You represent and warrant that:

(a) you have the authority to provide Personal Information to Blackboard, or to permit Blackboard to collect directly, for its use in accordance with the Agreement; and

(b) you have obtained and provided all required consents and/or disclosures to Authorized Users regarding Blackboard's collection, access and Processing of Personal Information under this Agreement, including to the extent applicable, to permit Blackboard to collect Personal Information directly from students under age 13 as permitted under the Children's Online Privacy and Protection Act ("COPPA").

4.4 To the extent necessary to provide you with the Products and Services, you authorize us, our affiliates and subsidiaries to Process Personal Information and you will facilitate a reasonable method for us to obtain such information, for example via secure transfer from and/or authorized access to your student information systems.

4.5 Where Blackboard discloses our employees' or contractors' Personal Information to you or a Blackboard employee/contractor provides their Personal Information directly to you, which you Process to manage your use of the Products and Services, you will Process that Personal Information in accordance with your data privacy policies and Applicable Data Privacy Laws. We will only make such disclosures where lawful for the purposes of managing your use of the Products and Services.

5. **Cooperation**

5.1 We will, to the extent legally permitted, promptly notify you if we receive an Individual Right Request. Our response to an individual Right Request will be limited to explaining to the individual that the Individual Right Request needs to be addressed to you.

If you do not have the ability to address an Individual Right Request directly through our Products and Services, we will upon your request assist you in responding to the Individual Right Request for the fulfilment of your obligation under Applicable Data Privacy Laws.

5.2 Unless legally prohibited, we will make available to you any information you request and otherwise reasonably assist you as necessary to demonstrate compliance with your obligations under Applicable Data Privacy Laws in relation to Personal Information (including obligations under Art. 35 and 36 GDPR).

6. **Third Party Access (Sub-processors)**

6.1 We shall not sell, disclose, release or otherwise transfer Personal Information to any third party without consent from you or an Authorized User, except where such disclosure is permitted (i) to a Sub-processor that Processes Personal Information on our behalf in support of Blackboard's Processing of Personal Information in accordance with Section 3.1 or 3.2, (ii) to a third party as reasonably necessary to comply with any applicable law, regulation, or public authority, (iii) to respond or participate in judicial process or to protect the safety of Blackboard or our users, or (iv) as otherwise permitted by Applicable Privacy Laws.

6.2 The list of Blackboard's current Sub-processors is available at https://blackboard.secure.force.com/btbb_articleview?id=kA53900000001LM. Subject to Clause 6.3, you hereby give us a general authorisation to engage the Sub-processors listed here.

6.3 We shall:

(a) inform you of any intended changes concerning the addition or replacement of Sub-processors at the link in Section 6.2 above (in combination with our email notification mechanism available at the link) thirty (30) days prior to any changes; and

(b) give you the opportunity to raise reasonable objections to such changes within twenty (20) calendar days of such notification. We may add or replace a Sub-processor immediately if it is necessary to ensure business continuity and recovery in case of emergency, except as prohibited by Applicable Data Privacy Laws.

6.4 With regard to our Sub-processors we will:

(a) conduct due diligence on the data privacy and security measures of new Sub-processors before providing access to Personal Information;

(b) enter into a written agreement which requires at least the same level of protection for Personal Information and individuals as set out in this DPA before providing access to Personal Information;

(c) restrict the Sub-processor's access to Personal Information only to what is necessary to fulfil our contractual obligations or as otherwise permitted under the Agreement or under Applicable Data Privacy Laws; and

(d) remain liable for any processing of Personal Information carried out by Sub-processors to the same extent we would be liable if performing the Services ourselves.

7. **Customer-Requested Third Party Access**

7.1 You acknowledge that in the provision of some of our Products and Services such as third party integrations, we, as authorized and instructed by you (or by your Authorized User who is eligible to provide such authorization under applicable law), may disclose Personal Information to and otherwise interact with a third party that acts on your behalf and under your instruction ("Third Party Data Processor"). You agree that if and to the extent such disclosures occur, between you and us, you are responsible for (i) meeting any requirements under Applicable Data Privacy Laws and the consequences of disclosing the Personal Information to the Third Party Data Processor, and (ii) for entering into separate contractual arrangements with such Third Party Data Processors binding them to comply with obligations in accordance with Applicable Data Privacy Laws. For the avoidance of doubt, such Third Party Data Processors are not our Sub-processors.

8. **Personal Information Hosting and Access**

8.1 Generally, Blackboard has a regional hosting model. For example, in the United States, all Personal Information is hosted in the United States. For support, development, maintenance

and similar purposes, your Personal Information may be accessed outside of the country in which it was originally collected.

8.2 If your Products and Services are not hosted regionally, you acknowledge and agree that to deliver the Products and Services and for support, development, maintenance and similar purposes, Personal Information may be Processed in countries other than the country in which it was collected. However, we will not Process Personal Information outside of the country it was collected unless such access meets the requirements under Applicable Data Privacy Laws. For sake of clarity, regardless of where we Process Personal Information, all Processing will be carried out in accordance with this DPA.

9. **EEA Personal Information Transfers**

9.1 If you are located in the EEA, we will not transfer Personal Information to any country outside the EEA which has not been the subject of a European Commission adequacy decision unless we have ensured that such a transfer adequately protects Personal Information and is made pursuant to an appropriate legal transfer mechanism, such as a valid certification under the EU-US Privacy Shield Framework, EU Commission approved Standard Contractual Clauses, Binding Corporate Rules, or any other legal transfer mechanism. To the extent that the legal transfer mechanism relied on is declared invalid (by, for example, a competent court or authority), we will cooperate with you in good faith to implement an alternative legal transfer mechanism.

10. **Security**

10.1 Annex B describes our technical and organizational security measures. The security measures are subject to technological advancements and further development. We are permitted to implement suitable alternative measures, as long as the alternative measures do not materially decrease the level of security applied to the Personal Information and meet the requirements of Applicable Data Privacy Laws.

10.2 We will regularly audit and assess our compliance with the technical and organizational security measures.

10.3 You are responsible for the appropriate use of the security features and other features of our Products and Services by you and your Authorized Users, including the granting of access entitlements. You are responsible for determining whether our Products and Services (including any test and staging environments) and the related security measures are sufficient for the intended Processing of Personal Information before using these Products and Services. We will provide you with any information that is reasonably required to make this determination.

11. **Security Incident**

11.1 Blackboard maintains a documented security incident response plan which is regularly tested.

11.2 Upon becoming aware of a Security Incident, we will (i) promptly investigate such Security Incident in accordance with our security incident response plan, (ii) take all measures and actions as are reasonably necessary to remedy or mitigate the effects of such Security Incident, and (iii) notify you promptly and without undue delay (and in any event within the time period required by applicable law) in writing upon confirmation of a Security Incident where an unauthorized party has acquired, accessed, or been disclosed Personal Information or as otherwise required by Applicable Data Privacy Laws ("Confirmed Security Incident").

11.3 In the event of a Confirmed Security Incident, we will:

(a) provide timely cooperation and assistance as you may require to fulfil your Security Incident reporting obligations under Applicable Data Privacy Laws.

(b) assist you in relation to any Security Incident notifications you may be required to make under applicable law. To the extent such information is available and required by law, the notification under Section 11.2 shall include the following:

(i) a general description of the Security Incident, including the nature and date of the Security Incident;

(ii) the categories and approximate number of individuals concerned;

(iii) the categories and approximate number of Personal Information records concerned;

(iv) the likely consequences of the Security Incident;

(v) the measures used to protect the Personal Information

(vi) the measures we have taken or propose to take to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects;

(vii) The name and contact details of our relevant point of contact with regard to the Security Incident.

(c) Upon request, provide reasonably requested information about the status of any Blackboard remediation and restoration activities and keep you informed about all material developments in connection with the Security Incident.

11.4 In the event of a Confirmed Security Incident, you will be responsible for the timing, content, and delivery of any legally required notification to your Authorized Users who are impacted by such Confirmed Security Incident and to any regulator or third party in accordance with applicable law. If, due to a Confirmed Security Incident which results from a breach of the data security obligations set forth in Annex B by Blackboard, its agents, or Sub-processors acting on its behalf, any third-party notification is required under applicable law, Blackboard shall, subject to the limitations of liability in the Agreement, reimburse you for all reasonable "Notification Related Costs." Notification Related Costs are limited to internal and external costs associated with addressing and responding to the Confirmed Security Incident, including but not limited to: (a) preparation and mailing or other transmission of notifications required by applicable law; (b) establishment of an adequate call center and other communications procedures in response to the Confirmed Security Incident; (c) costs for remediation measures such as credit monitoring or reporting services for affected individuals for at least twelve (12) months in relation to a Security Incident that involves social security numbers, or to the extent required by law. With respect to any Security Incident which does not result from a breach of the data security obligations set forth in Annex B by Blackboard, its agents, or Sub-processors acting on its behalf, any third-party notifications, if any, shall be at your expense.

11.5 Blackboard's obligation to report or respond to a Confirmed Security Incident under this Section 11 is not and will not be construed as an acknowledgement by Blackboard of any fault or liability of Blackboard with respect to the Confirmed Security Incident.

11.6 Unless prohibited by law, you will notify us before communicating the Confirmed Security Incident to a third party (whether to any regulators, Authorized Users, clients, or the public) and provide us with copies of any written documentation to be filed with the regulators and of any other notification you propose to make which references us, our security measures and/or role in the Confirmed Security Incident, whether or not by name. Subject to your obligations to comply with any mandatory notification deadlines under Applicable Data Privacy Laws, you will consult with us in good faith and take account of any clarifications or corrections we

reasonably request to such notifications or communications and which are consistent with Applicable Data Privacy Laws.

12. **Audit**

12.1 We will, by way of regular self-audits, verify that the Processing of Personal Information complies with Applicable Data Privacy Laws.

12.2 Subject to Clause 12.3, we will allow for and contribute to audits, including inspections, conducted by you or another auditor mandated by you regarding our compliance with the DPA and Applicable Data Privacy Laws.

12.3 To fulfil our obligations under 12.2, we will provide you, upon request, an overview of our privacy and security program, governance and controls including:

(a) overview of our privacy program and governance;

(b) overview of our security program and governance;

(c) overview of security controls regarding a specific Product or Service (where available);

(d) summaries of any relevant self-audits;

(e) summaries of any relevant third party assessments or reports (where available);

(f) relevant security reports and/or certifications of our data centers (where available);

(g) description of our processes for assistance with Individual Rights Requests; and

(h) certified statement on the compliance with this DPA.

12.4 If, after review of the documentation provided in accordance with Section 12.3, you require further information to meet your obligations under Applicable Data Privacy Laws, you may:

(a) request further information with an explanation regarding what further information is required and why it is required; and

(b) no more once per year, request an on-site audit where Applicable Data Privacy Laws grant you the right to conduct an on-site audit.

12.5 You will reimburse us for reasonable expenses for any time expended for any such on-site audit. Requests need to be made at least 14 days in advance in writing, and we will mutually agree upon the scope, timing, and duration of the on-site audit

12.6 Any information made available in accordance with this section 12 shall be deemed Confidential Information. You will promptly notify us regarding any possible non-compliance discovered during the course of an audit, and we will use commercially reasonable efforts to address any confirmed non-compliance as soon as practicable.

13. **Deletion or return of Personal Information**

13.1 Upon expiration or termination of the Products or Services, or such earlier time upon request, we will delete the relevant Personal Information in our possession, custody or control within a reasonable time and procure the deletion of all copies of Personal Information processed or maintained by any Sub-processors. At your request and your expense, we will return such Personal Information to you before deleting it, provided that a request for the return of Personal Information is submitted to Blackboard in writing at least thirty (30) days prior to the date of termination. If no such request for the return of Personal Information is received, Blackboard may, but shall have no obligation to, maintain or return Personal Information more

than 10 days after the termination of the Products or Services. We will certify the deletion of Personal Information upon request.

13.2 Notwithstanding the foregoing, we may retain Personal Information to the extent: (i) required by applicable laws; (ii) required as part of our automated backup and recovery processes so long as the backup and recovery storage system is inaccessible to the public and unable to be used in the ordinary course of business by Blackboard; (iii) an Authorized User has downloaded, saved, transferred or otherwise maintained their own personal information in a personal account in accordance with Section 4.3; and/or (iv) it is aggregated or De-Identified Data and Blackboard has implemented technical safeguards and business processes to prohibit the reidentification of the information with an individual. If you request deletion of Personal Information in archival and back-up-files, you shall bear the costs including costs for business interruptions associated with such request.

14. **Final provisions**

14.1 Unless specifically stipulated to the contrary by the Parties, the duration of this DPA will be coterminous with the term of the Agreement. Our obligations under the DPA will continue to apply as long as we Process Personal Information.

14.2 This DPA is incorporated into and made a part of the Agreement by this reference and replaces any arrangements agreed earlier between the parties in respect of the Processing of Personal Information related to the Agreement. In the event of a conflict between this DPA and any other provision of the Agreement between you and us, this DPA will prevail; provided that if you and we have agreed in an Order Form to any terms that are different from this DPA, the terms in such Order Form will prevail.

14.3 Notwithstanding any notice requirements in the Agreement, we may update this DPA from time to time to better reflect changes to the law, new regulatory requirements or improvement to the Products and Services. The updated Terms shall be posted here: http://agreements.blackboard.com/bbinc/data-processing-addendum.aspx. If any update to the DPA constitutes a material change to the ways in which we Process Personal Information, or materially affects your use of the Products and Services or your rights herein, we will provide notice a minimum of 30 days prior to the changes taking effect. Your continued use of the Service thereafter shall constitute acceptance to be bound by the updated DPA.

Annex A – Details of Processing

This Annex A describes the Processing of Personal Information as required under GDPR.

The details of the Processing depend on your use of our Products and Services but will generally be as follows:

Categories of Personal Information

- Name or unique identifiers
- Personal contact information and information about role at institution
- Date of birth, gender, nationality, parent/student relationships
- Course and degree information such as grade level, teachers, classes/sections/courses, grades, assignments, tests, books, attendance, homework, degree type
- Access credentials usernames and passwords
- Information related to the devices accessing our Products and Services, service or browsing history, location data, information provided by social networks, Authorized User or Customer correspondence
- Disciplinary and conduct records
- Personal information contained in content generated and/or provided by an Authorized User such as submitted papers, assignments, blog and discussion posts, contributions to online collaboration such as chats and audio/video conferencing

Special Categories of Personal Information (if any)

Our Products and Services are generally not intended to Process Special Categories of Personal Information. Any Processing of Special Categories of Personal Information is determined and controlled by you in compliance with Applicable Data Privacy Laws.

Special Categories of Personal Information may include: (a) Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (b) genetic data and biometric data Processed for the purpose of uniquely identifying an individual; and (c) data concerning health or data concerning an individual's sex life or sexual orientation.

Categories of Data Subject

Customer’s representatives (such as employees, contractors, consultants and agents) and Customer’s Authorized Users (such as students, prospective students, parents, teachers and administrators), guest users invited by Customer or its Authorized Users.

Purpose and nature of Processing

As a provider of education technology solutions, we Process Personal Information provided by you or your Authorized End Users on your behalf and under your instructions within the scope of the Agreement. Processing operations may include storage and other Processing necessary to provide our Products and Services and otherwise perform our obligations as described in Section 3.

Annex B – Security measures

We use the following appropriate technical and organizational measures to protect Personal Information which have to meet, at a minimum, the level required by applicable law:

Management controls

- We maintain a comprehensive information security program with an appropriate governance structure (including a dedicated Information Security team) and written security policies to oversee and manage risks related to the confidentiality, availability and integrity of Personal Information.

- We align our information security program and measures with industry best practices, such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, Open Web Application Security Project (OWASP), and National Institute of Standards and Technology (NIST) 800 frameworks. These controls are distilled and incorporated into an internal compliance framework that is applicable to all Products and Services.

- We use internal resources and third-party contractors to perform audits and vulnerability assessments and provide guidance on best practices for select systems containing Personal Information. System assessments and network audits are performed regularly. Issues identified during audits are prioritized and remediated as part of ongoing security monitoring using a risk management methodology.

- Our employees receive security and data privacy training when they start and regularly thereafter. Awareness campaigns are used to raise awareness about information security risks and our information security policies and procedures. Select staff, such as developers, receive additional security training tailored to their job role. Completion of training is tracked.

- New employees undergo background checks prior to onboarding, where permitted by applicable law, and sign a confidentiality agreement.

- Employees are required to comply with internal policies on the acceptable use of corporate IT assets. These policies address requirements on clean desk and secure workspaces, protecting system resources and electronic communications, protecting information, and general use of technology assets. Our employees are made aware that non-compliance with these policies can lead to disciplinary action, up to and including termination of employment/contract.

- We maintain a vendor risk management program to manage the security and integrity of our supply chain. Our procurement process for third party service providers that have access to confidential information (including Personal Information) includes a vendor security and privacy assessment review and a contract review by our Legal team.

- We have a documented security incident response process for responding to, documenting, and mitigating Security Incidents and notifying our clients, authorities or other parties as required. The process is tested regularly.

Admission control

- We employ appropriate physical safeguards to prevent unauthorized persons from gaining access to the premises where Personal Information is collected, processed and used. Such premises may only be entered by us and/or our agents.

- We and our service providers implement physical security controls for the data centers used to store Personal Information. These controls are commensurate with industry best practices and local regulations, which include 24x7x365 video monitoring, guards, secured ingress/egress, badged access, sign-in/sign-out logs, restricted access, and other best practices.

- We use appropriate measures to secure buildings, such as using access cards or fobs for employee access.

- We use appropriate measures to ensure that Personal Information held in hardcopy are kept securely e.g. in locked rooms or filing cabinet. Generally, steps are taken to ensure that access to hardcopy Personal Information is limited in the same way it would be on an electronic IT system i.e. access is limited to those individuals where it is necessary for them to have access in order for them to perform their job role.

Entry control

- We use appropriate measures to prevent unauthorized parties from accessing or using our systems containing Process Personal Information.

- We require authentication and authorisation to gain access to systems that Process Personal Information (i.e. require users to enter a user id and password before they are permitted access to such systems).

- We have procedures in place to permit only authorized persons to access Personal Information internally or externally by using authentication procedures (e.g. by means of appropriate passwords), except as otherwise enabled by you.

Access control

- We employ appropriate measures to prevent individuals accessing Personal Information unless they hold a specific access authorization.

- We only permit access to Personal Information which the employee (or agent) needs for his/her job role or the purpose they are given access to our systems for (i.e. we implement measures to ensure least privilege access to systems that Process Personal Information). System administration and privileged access is controlled and enforced on a need-to-know basis and is reviewed regularly.

- We have in place appropriate procedures for controlling the allocation and revocation of access rights to Personal Information. For example, having in place appropriate procedures for revoking employee access to systems that Process Personal Information when they leave their job or change role. Unnecessary and default user accounts and passwords are disabled on servers.

- Our systems containing Personal Information are protected by user identifiers, passwords and role-based access rights. Special access rights are produced for the purposes of technical maintenance which do not allow access to Personal Information.

- We implement methods to provide audit logging to establish accountability by monitoring network devices, servers, and applications. Where applicable, aberrant activity generates alerts for investigation and/or action.

- All employees must use multi-factor authentication for remote access to IT assets within the corporate network.

- We take appropriate administrative safeguards to protect our services against external attacks, including, for example, deploying firewalls and using services to provide 24x7x365 security monitoring of our data centers to protect and defend against external security threats.

Transmission control

- We employ appropriate measures to protect the confidentiality, integrity and availability of Personal Information during electronic transmission.

- We encrypt Personal Information while in transit over the internet.

Input control

- We maintain logging and auditing systems to monitor activity related to the input of Personal Information

Order control

- We ensure that all requests from you with respect to Personal Information are processed strictly in compliance with your instructions through the use of clear and unambiguous contract terms; comprehensive Statements of Work; appropriately designed policies and processes, and training.

Availability control

- We protect Personal Information in our possession against unintentional destruction or loss by implementing appropriate management, operations, and technical controls such as firewalls; monitoring; and backup procedures.

- Example measures that may also be taken include mirroring of storage media, uninterruptible power supply (UPS); remote storage; and disaster recovery plans.