Data Security Addendum

BigRedSky Pty Ltd (ACN 692 733 716)

Version: 1 – January 2026

This Data Security Addendum (the "**Addendum**") amends the Agreement between BigRedSky Pty Ltd (ACN 692 733 716) and Customer and sets out the obligations of both parties regarding the security of Your Data in connection with the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum will take precedence only with respect to the security of Your Data. Customer will be the same as "Customer", "Client", or "you"; and BigRedSky will mean the same as "us", "we", "BRS" or "BigRedSky", as the terms may be used in the Agreement.

1. DEFINITIONS

a. "**Agreement**" means the underlying agreement between BRS and Customer for the provision of Services that references and incorporates this Addendum.

b. "**Business Continuity and Disaster Recovery Plan**" means a business continuity, contingency and disaster recovery activation plan to minimize disruption in and reinstate the operation of the use of the Services by you due to a disaster or similar event.

c. "**Documentation**" means manuals, handbooks, guides and other user instructions, documentation and materials available through the Services or provided by us regarding the capabilities, operation, and use of our Services.

d. "**Professional Services**" means the implementation, customization, training, consulting or other professional services we provide, as may be described in the applicable Agreement.

e. "**Property**" means our property, which includes but is not limited to our Services, information, Documentation, data (whether tangible or intangible) and Usage Information. Property also includes data, information and technologies supplied by our third-party providers and available through the Services.

f. "**Security Breach**" means a confirmed breach of security that results in the unauthorized destruction, loss, alteration, disclosure of, or access to Your Data where such breach of security is likely to result in a significant risk of harm to you or your Data or where BRS is required by applicable data protection law to notify you thereof.

g. "**Services**" means the cloud computing services, software-as-a-service, online research services, Professional Services, as well as any products, including installed software, supplied by BRS that are detailed in the applicable Agreement.

h. "**Usage Information**" means any information, data, or other content (including statistical compilations and performance information) related to or derived from your access to and use of the Property.

i. "**Your Data**" means, other than Usage Information, information, data, and other content, in any form or medium, that is submitted, posted, or otherwise transmitted by you or on your behalf through the Services.

2. INFORMATION SECURITY PROGRAM

a. BRS will maintain an information security program that adopts the International Organization for Standardization (ISO/IEC 27001:2022. The program will include, but is not limited to, the following components:

   i. Information security policy framework;

   ii. Program documentation;

   iii. Auditable controls;

   iv. Compliance records; and

   v. Appointed security officer and information security personnel.

b. BRS will establish and maintain information security policies designed to protect the confidentiality and integrity of Your Data hosted in the Services, which will include the following:

   i. Policies to restrict access to Your Data only to authorized BRS personnel and subcontractors;

   ii. Policies requiring the use of user IDs, passwords, and multi-factor authentication to access Your Data;

iii. Policies requiring connections to the internet to have commercially reasonable controls to help detect and terminate unauthorized activity prior to the firewall maintained by BRS;

iv. Policies requiring performance of periodic vulnerability assessments;

v. Policies for the use of anti-malware and patch management controls to help protect against virus or malware infection and exploitation of security vulnerabilities; and

vi. Policies and standards for the use of auditable controls that record and monitor activity.

c. BRS will train and communicate to BRS personnel its defined information security principles and information security policies and standards in accordance with the following:

i. Applicable BRS personnel will be required to take training, both at hire and on a regular basis, in information security practices and the correct use of information processing facilities to minimize possible security threats; and

ii. Applicable BRS personnel will be instructed to report any observed or suspected threats, vulnerabilities, or incidents to BRS management to deal with appropriately.

d. BRS will be responsible for its personnel's compliance with the terms of the Agreement and with BRS standard policies and procedures. BRS will maintain a disciplinary process to address any unauthorized access, use, or disclosure of Your Data by any BRS personnel.

e. BRS will maintain a formal plan for incident response to promptly respond to suspected or confirmed breaches of Your Data in accordance with regulatory and legal obligations.

f. BRS policy with respect to user IDs and passwords for BRS personnel accessing BRS systems includes, but is not limited to, the following components:

i. Each user has a unique account identifier or user ID;

ii. Each user ID or account is assigned a password;

iii. User IDs are added, modified, and deleted in accordance with BRS-approved account management processes;

iv. Verification of user identify before password resets;

v. Passwords must conform to defined criteria that included length, complexity requirements and limitations on reuse;

vi. User IDs, passwords and tokens are not shared or used by anyone other than the user to whom it was assigned;

vii. Temporary or default passwords are set to unique values and changed after first use;

viii. User ID password changes are required at least every ninety (90) days;

ix. Failed and repeated access attempts are locked for a reasonable and appropriate duration;

x. Idle sessions are locked after a commercially reasonable period of time; and

xi. User IDs are disabled after personnel termination.

3. DATA SECURITY CONTROLS

Application Strategy, Design and Acquisition

a. BRS will review applicable applications and network components and assess their business criticality.

b. BRS will review critical applications regularly to ensure compliance with industry and commercially reasonable security standards.

Anti-Virus and Anti-Malware

c. BRS will implement and configure industry standard anti-virus and anti-malware software on systems holding or processing Your Data for regular signature updates.

d. BRS will implement threat management capabilities designed to protect systems holding or processing Your Data.

Network Security

e. BRS will configure network devices (including routers and switches) according to approved lockdown standards.

f. BRS will implement logical network segmentation within its AWS environment, using separate VPCs and subnets, and will apply network security controls approved by its authorised security personnel.

Web and Application Security

g. BRS will maintain commercially reasonable security measures for internet-accessible applications, including:

   i. Implementing processes for developing secure applications;

   ii. Performing pre-deployment and ongoing security assessments of internet-accessible applications;

   iii. Developing internet-accessible applications based on secure coding guidelines such as those found in the Open Web Application Security Project ("OWASP") Development Guide; and

   iv. Validating the input, internal processing, and output of data in internet-accessible application(s).

h. BRS implement a change management process for documenting and executing operational changes in Services.

Compliance

i. BRS will establish and adhere to policies that comply with laws and regulations that are applicable to BRS and its provision of Services. BRS does not determine whether Your Data includes information subject to any specific law or regulation and compliance with any such law or regulation is the sole responsibility of the Customer.

j. To the extent legally permitted, BRS will endeavor to notify the Customer promptly after BRS receives correspondence or a complaint from a government or regulatory official or agency related to the security of Your Data. For purposes of the foregoing, a correspondence or complaint excludes normal customer service correspondence or inquiries.

Physical and Environmental Security

k. BRS Services are hosted within Amazon Web Services ("AWS") facilities, which are protected by AWS's industry-standard physical, environmental, and security controls. These controls ensure the confidentiality, integrity, and availability of systems that store or process BRS data. Accordingly: Such BRS facilities will be physically protected from unauthorized access, damage, and interference;

   i. AWS data centres are physically protected from unauthorized access, damage, and interference through layered security measures including staffed security, video surveillance, intrusion detection, and access-logging systems.

   ii. All physical access to AWS data centres is logged, monitored, and routinely audited by AWS security operations teams providing global, 24/7 support.

   iii. AWS maintains strict visitor and contractor procedures, including identity verification, escorted access, and restrictions that allow entry only to authorised areas.

   iv. AWS employs extensive physical safeguards and environmental controls, including fire detection and suppression systems, redundant power infrastructure, and climate management designed to protect systems from security threats and environmental hazards.

Security Testing and Patching

l. BRS will perform security testing for common security coding errors and vulnerabilities against systems holding or processing Your Data in line with generally accepted industry standards.

m. BRS will regularly scan systems holding or processing Your Data for security vulnerabilities.

n. BRS will follow a commercially reasonable and industry standard security patching process.

Exchange, Transfer, and Storage of Information

o. BRS shall ensure that all account usernames and authentication credentials are stored and transmitted across networks and protected with a minimum of 128 AES encryption. BRS shall not store user credentials in clear text under any circumstances. Your Data shall be encrypted at a minimum of 128 AES when in transit and 256 AES at rest. BRS will also use encryption for Your Data being transmitted across the public Internet or wirelessly, and as otherwise required by applicable laws. BRS will hold such encryption keys in the strictest of confidence and limit access to only named individuals with a need to have access.

p. Your Data will not be stored or transported on a laptop or any other mobile device or storage media, including USB, DVDs, or CDs, unless encrypted using a commercially reasonable encryption methodology. All electronic data transfers of Your Data by BRS will be transmitted via SFTP or other commercially reasonable encrypted form.

Penetration Testing, Monitoring, Vulnerabilities

q. BRS or an appointed third party may periodically perform penetration testing on the BRS systems supporting the Services. Upon written request, BRS shall make available to Customer a summary on the outcome of such relevant penetration testing or an executive summary of the penetration testing results.

r. BRS will monitor the relevant BRS information systems for security threats, misconfigured systems, and vulnerabilities on an ongoing basis.

s. BRS will classify any vulnerability findings identified as emergency, critical, high, medium, or low in accordance with generally accepted industry standards for providers of similar services, and in accordance with BRS risk assessment policies. Although the actual timeframe needed to affect such remediation will depend on the nature of the finding, BRS will undertake commercially reasonable efforts to correct vulnerabilities according to the following timeframes:

Vulnerability Classification	Definition	Remediation Goal
Emergency	A vulnerability that has a high probability of being widely exploited in a manner disruptive to normal business operations	Begin deployment of patches and mitigations promptly, without undue delay, and complete remediation activities within seven (7) days
Critical	A vulnerability that has a high probability of being exploited that could result in broad exposure of confidential information or disruption of service, but the nature of the vulnerability does not reach the level of an “emergency” risk	Without undue delay and in any event within thirty (30) days
High Risk	A vulnerability that has a reasonably high probability of being exercised that could allow broad exposure or compromise of confidential information or disruption of service.	Without undue delay and in any event within sixty (60) days
Medium Risk	A vulnerability that has a medium probability of being exercised.	Without undue delay and in any event within ninety (90) days
Low Risk	A vulnerability that has a low probability of being exercised.	Best efforts to address vulnerability in accordance with BRS risk management policies. Depending on the scope of the vulnerability, correction may be addressed in the next scheduled update.

Personnel Access

t. BRS will implement controls designed to manage its personnel’s access to systems supporting the Services to be granted on a need-to-know basis consistent with assigned job responsibilities, which may include the use of role-based access controls to help ensure appropriate access rights, permissions, and segregation of duties.

Segregation of Data

u. BRS agrees that Your Data hosted within the Services in a production environment is maintained so as to preserve logical segregation of Your Data from data of others.

Data Removal, Deletion and Destruction

v. If not otherwise set forth in the applicable Agreement, upon conclusion or termination of the Services at the written request of the Customer, BRS will securely destroy and, upon request, confirm the destruction of all copies of Your Data in any electronic or non-electronic form, except (i) for backup or archival copies kept in the normal course of business, including as part of a defined data retention program; or (ii) to the extent necessary to comply with applicable law and regulations.

Adjustment of Data Security Controls

w. BRS will evaluate and may adjust its data security controls in light of: (i) the results of the testing monitoring; (ii) any material changes to BRS operations or business arrangements; (iii) the results of risk assessments performed; or (iv) any other circumstances that BRS knows or has reason to know may have a material impact on its data security controls.

4. NOTIFICATION OF SECURITY BREACH

a. BRS will, without undue delay but in any event within seventy-two (72) hours of discovery, notify Customer of a Security Breach. BRS agrees that it will not inform any third party of any Security Breach naming you without first obtaining Customer's prior written consent, unless if (i) required by applicable law or regulation; or (ii) such disclosure is in furtherance of a BRS security breach investigation or the execution of its response plan.

b. In the event of any such Security Breach, BRS will take commercially reasonable measures and actions to remedy or mitigate the effects of the Security Breach and will perform a root cause analysis to identify the cause of such Security Breach.

c. Upon Customer's reasonable request, BRS may provide documentation related to such Security Breach, including, to the extent known, a summary of the cause of such Security Breach and steps taken to remedy the Security Breach and to prevent a reoccurrence. BRS will reasonably cooperate with Customer in seeking injunctive or other equitable relief against any third party deemed responsible or complicit in the Security Breach.

d. If legally permitted, in the event of a Security Breach, BRS agrees to reasonably cooperate with Customer with protecting its rights relating to the use, disclosure, protection, and maintenance of Your Data.

5. SERVICES RESILIENCE

a. BRS will use commercially reasonable efforts to restore the Services by having offline backups of application data, infrastructure components and configuration settings.

b. BRS will use commercially reasonable efforts to protect Services that host or process Your Data against denial-of-service attacks by implementing denial-of-service mitigation solutions.

6. SHARED SECURITY OBLIGATIONS

You agree that you are responsible for all transactions that occur on your account and that it is your responsibility to ensure that you and your users use unique usernames and strong passwords for each account used to access the Services. You agree that you and your users must hold in confidence all usernames and passwords used for accessing the Services, and each user must immediately change their username/password combinations that have been acquired by or disclosed to an unauthorized third party. You also agree to enroll and require your personnel and other users to enroll in multi-factor authentication ("MFA") where made available to you, and you are responsible for all transactions and other activity that would have been prevented by the proper use of MFA. Additionally, you will notify BRS if you become aware of any unauthorized third-party access to BRS data or systems and will use reasonable efforts to remedy identified security threats and vulnerabilities to your systems.

7. BACKGROUND CHECKS

Employment background checks serve as an important part of BRS selection process. Verifying background information validates a candidate's overall employability or an employee's suitability for a particular assignment. Depending on the country and position at issue, to the extent as is customary and permitted by law, all BRS background checks may include

identification verification, prior employment verification, criminal background information, global terror/sanctions checks and education verification. BRS agrees to use qualified information security personnel to perform data security services.