Andeavour Security Measures Addendum
To Customer Data Processing Agreement
(Andeavour as Supplier)

As of the Effective Date of the DPA between Andeavour and Customer, Andeavour will implement and maintain the Security Measures set out in this Addendum. "DPA" refers to the Andeavour Customer Data Processing Agreement (Andeavour as Supplier), available at www.andeavour.com/data-processing-agreement.pdf, or any superseding signed data processing or protection agreement in effect between Andeavour and Customer. Andeavour reserves the right to complete the implementation of the Security Measures outlined in this Addendum at any time during 2025–2026, at its sole discretion. Andeavour may update this Addendum by publishing a revised version at www.andeavour.com/security-measures-addendum.pdf.

Security Control Category	Description
1. Governance	a. Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing Andeavour's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data b. Use of data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions
2. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur c. Document formal risk assessments d. Review formal risk assessments by appropriate managerial personnel
3. Information Security Policies	a. Create information security policies, approved by management, published and communicated to all employees and relevant external parties b. Review policies at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness
4. Human Resources Security	a. Maintain policies requiring reasonable background checks of any new employees b. Regularly and periodically train personnel on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization
5. Asset Management	a. Maintain policies establishing data retention and secure destruction requirements
6. Access Controls	a. Maintain controls designed to limit access to Personal Data b. Review personnel access rights on a periodic basis c. Maintain policies requiring termination of physical and electronic access to Personal Data after termination of an employee d. Implement access controls designed to authenticate users and limit access to Personal Data

	e. Maintain dual layer access authentication processes for Andeavour employee access to Andeavour systems
7. Cryptography	a. Implement encryption key management procedures b. Encrypt sensitive data using a minimum of AES-256 bit ciphers in transit
8. Communications Security	a. Maintain a secure boundary using firewalls and network traffic filtering b. Require segmentation to isolate production systems from development systems c. Require periodic reviews and testing of network controls
9. System Acquisition, Development, and Maintenance	a. Assign responsibility for system security, system changes and maintenance b. Test, evaluate and authorize major system components prior to implementation
10. Supplier Relationship	a. Periodically review available security assessment reports of Sub-processors to assess their security controls and analyze any exceptions set forth in such reports
11. Information Security Incident Management	a. Monitor the access, availability, capacity and performance of system logs and network traffic b. Maintain incident response procedures for identifying, reporting, and acting on Information Security Incidents c. Establish a cross-disciplinary Security Incident response team
12. Business Continuity Management	a. Implement a tiered data architecture with operational diversity to allow rapid recovery in the event a service impacting incident b. Establish procedures designed to ensure all applicable statutory, regulatory and contractual requirements are adhered to

v.2024.03.21