Business Conduct Requirements

1. Definitions and interpretation

Capitalized terms used but not defined in these Business Conduct Requirements ("Requirements") shall have meanings assigned in other Contract Documents.

Anti-corruption Law means any anti-bribery and anti-corruption Law applicable to either Party or the Contract.

Applicable Trade Control Law means any Trade Control Law applicable to either Party.

Bribe means any offer of, payment of, or request for, any monetary or other thing of value to influence a Government Official or any other person to act improperly in performing his/her duties. This includes giving of a facilitation payment, which is a payment or gift, even if small, to a Government Official to speed up his/her performance of a routine and non-discretionary service.

Code means Company's Code of Business Conduct accessible on the 'Suppliers' section of Company's website, as updated from time to time.

Company means South32 Hermosa Inc.

Company Data has the meaning in clause 5(b) of these Requirements.

Company Personal Information means all Personal Information provided or made available by or on behalf of Company or that is otherwise generated or collected by Contractor in connection with performance of this Contract.

Contractor means the counterparty to Company under the Contract.

Data Breach means any incident involving interference with or misuse, loss, or unauthorized Processing of Company Personal Information.

Data Privacy Law means all current or future Law relating to data protection, privacy and information security which apply to either Company or Contractor in connection with this Contract.

Government Official includes any:

(a) officer, employee or agent of a government or public international organization or any department or agency thereof or any government-owned or controlled entity (including state owned or controlled enterprises);

(b) political party or party official, or political office candidate; and

(c) person acting on behalf of such government or public international organization, or any agency, department, or instrumentality thereof.

Modern Slavery means any activity, practice or conduct that would constitute an offense in relation to slavery, forced labor, child labor, forced marriage, involuntary servitude, debt bondage, human trafficking or other slavery-like exploitation under applicable anti-slavery and human trafficking Law, statutes, codes, and international conventions from time to time in force.

Personal Information means any information (including an opinion) about an identified or identifiable natural person, and includes any permitted purpose categories of data listed in the Privacy Policy.

Privacy Policy means Company's privacy policy, as set out on Company's website, as updated from time to time.

Process or **Processing** means any operation or set of operations which is performed upon Personal Information whether or not by automatic means, including collecting, recording,

organizing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing, and destroying such Personal Information.

Protected Data means Company Personal Information and Company Data.

Sanctioned Party means:

(a) any person or entity designated for export controls or sanctions restrictions under Applicable Trade Control Law including without limitation any designation under the United States List of Specially Designated Nations and Blocked Persons, the Sectoral Sanctions Identification List, the US Bureau of Industry and Security Entity List, the United Kingdom Consolidated list, the EU Consolidated List and Australia's Consolidated List; and/or

(b) any entity 50% or more owned, or controlled, directly or indirectly, by one or more of the foregoing persons or entities.

Sustainability Policy means the document of the same title accessible on the 'Suppliers' section of Company's website, as updated from time to time.

Trade Control Law means any economic sanctions, export control, customs or import Law, or other regulations, orders, directives, designations, licenses or decisions applicable to either Party or this Contract and relating to trade or transfer of goods, technology, software and/or services which are imposed, administered or enforced from time to time, including without limitation those established by Australia, United States, United Kingdom, Singapore, European Union, European Union Member States, or United Nations.

2. Supplier Business Conduct

(a) Contractor acknowledges it has access to a copy of, has read and will comply with, the Code, Sustainability Policy, and Privacy Policy as applicable from time to time, and it will ensure Contractor's Personnel performing Services or Work or providing Goods have read, understood, and will follow, the same.

(b) Contractor must be, and ensure all Contractor's Personnel are, aware of and comply with Site Standards and Procedures.

3. Anti-corruption Compliance

Contractor represents, warrants, and undertakes:

(a) neither Contractor nor any of Contractor's Personnel, directly or indirectly, has given or will give any Bribe to a Government Official or any person to obtain the award of this Contract or while this Contract is effective;

(b) save for any ownership interest in respect of shares on a recognized stock exchange, no officer, director, employee, or shareholder of Contractor is, or currently expects to become, a Government Official in a position to take or influence official action for or against Company during the term of this Contract;

(c) it will notify Company promptly, and in any event within 3 days, upon becoming aware any of its officers, directors, employees, or shareholders becomes, or expects to become, a Government Official in a position to take or influence official action for or against Company;

(d) if Contractor is to act, or may act, on Company's behalf (directly or via a third party) in dealing with Government Officials in supplying any Work, Goods, or Services under this Contract, Contractor must:

(i) obtain prior written permission from Company to do so; and,

(ii) perform appropriate anti-corruption due diligence on any such third party, keep records of the same and take reasonable measures to ensure such third party complies with clauses 3(a), 3(b), 3(c) and 3(d) of these Requirements; and,

(e) it will notify Company promptly upon becoming aware of any actual, suspected, or imminent breach of clause 3(a), 3(b), 3(c) or 3(d) of these Requirements by Contractor or Contractor's Personnel.

(f) Without limiting any other rights of Company at law or under this Contract, if Company reasonably suspects Contractor is in breach of or breached clause 3(a), 3(b), 3(c), 3(d), 3(e), 4, or 6 of these Requirements, or Company knows or reasonably suspects such a breach is imminent, then:

(i) Company may terminate this Contract or part thereof for cause by written notice to Contractor with immediate effect; and,

(ii) at Company's discretion, Company may terminate and/or cancel any claims for payment by Contractor in relation to this Contract.

4. Human Rights Compliance

(a) Contractor and Contractor’s Personnel must:

(i) not engage in any conduct inconsistent with recognized international human rights, including as outlined in the United Nations Guiding Principles on Business and Human Rights, and the Voluntary Principles on Security and Human Rights (and in the event of any ambiguity, discrepancy, or inconsistency in or between these documents, the highest standard applies);

(ii) not engage in Modern Slavery; and

(iii) ensure it has reasonable policies and reasonable processes in place to comply with clauses 4(a) and 4(b) of these Requirements at and in all of its operations and supply chains.

(b) Upon entering the Contract, and at any time during the term of the Contract when requested to do so in writing by Company, Contractor must:

(i) cooperate with any due diligence process being conducted by Company (or any third-party appointed by Company) of Contractor's operations or supply chains; and

(ii) provide any information reasonably requested by Company for this purpose.

(c) Contractor must notify Company promptly upon, and in any event no later than 3 days after, becoming aware of any actual or potential breach of clause 4(a) or 4(b) of these Requirements.

5. Privacy and Data Security

(a) Contractor must, in relation to all Company Personal Information:

(i) only Process such Company Personal Information in a manner consistent with the Privacy Policy and in accordance with instructions from Company;

(ii) provide any assistance reasonably requested by Company to enable Company to comply with all Data Privacy Law or to respond to requests or inquiries from relevant data subjects; and,

(iii) not store, transfer, or disclose any Company Personal Information outside the jurisdiction in which it was originally generated or collected by Contractor, except

with Company's express prior consent. If reasonably required by Company to support any storage, transfer, or disclosure of Company Personal Information in a different jurisdiction, Contractor will enter into a data processing agreement in a form provided by Company (where relevant based on standard provisions approved under Data Privacy Law).

(b) Where Contractor:

(i) has custody or control over any of Company's Confidential Information; or

(ii) is required to access, transmit or store Company's Confidential Information,

on or via networks or servers connected with Contractor's information systems or equipment ("Company Data"), Contractor must:

(iii) put in place and maintain appropriate technical and organizational measures to secure Company Data, having regard to risk of accidental or unauthorized access, loss, destruction, misuse, interference, modification, disclosure, or damage;

(iv) to give effect to the subclause above, take all reasonable measures to identify risk (internal and external) to safeguard Protected Data in its possession or under its control and regularly verify and update these safeguards against risk(s) identified;

(v) ensure its physical and technical security systems only permit properly authorized and trained Contractor's Personnel to access Protected Data;

(vi) no less than once per calendar year, provide appropriate training to Contractor's Personnel with respect to correct handling of Protected Data to minimize risk of a Data Breach;

(vii) comply with all security requirements, policies, procedures, or directions as specified in this Contract or notified by Company in writing from time to time;

(viii) if requested by Company, provide regular security assurance reports to Company, which include such information as is reasonably required for Company to assess performance of Contractor's obligations in relation to security of Protected Data;

(ix) on termination or expiry of this Contract, or upon written request at any time, cease and ensure Contractor's Personnel cease to use or process Protected Data and return and/or procure the return of any and all Protected Data in their possession or control to Company; and,

(x) upon request provide Company with all reasonable detail and written confirmation of Contractor's compliance with this clause 5(b).

(c) Contractor must ensure it does not, by any act or omission, adversely affect or alter the operation, functionality and technical environment of any information systems or equipment used to Process Protected Data, or Company's ability to access, modify or use any Protected Data, without prior written consent of Company.

(d) Contractor agrees not to modify any Protected Data under its control or possession, merge it with other data, commercially exploit or engage in any other practice or activity which may in any manner adversely affect the integrity, security, or confidentiality thereof, other than specifically permitted herein or as directed by Company in writing.

(e) If Contractor becomes aware of any actual or suspected:

(i) misuse, interference or loss or unauthorized access, modification, or disclosure of Protected Data by any person;

(ii) breach of Contractor's obligations in relation to Protected Data; or

(iii) event which results in an actual or potential adverse effect on any information systems or equipment used to Process Protected Data, or Company's ability to access, modify or use any Protected Data,

(in each case a “Data Breach”), Contractor must (at its own cost):

(iv) promptly (and in any event within 24 hours) report the Data Breach to Company;

(v) mitigate, to the extent practicable, any harmful effect of the Data Breach;

(vi) provide Company with all information relevant to the Data Breach reasonably available to Contractor;

(vii) provide any assistance reasonably requested by Company for purposes of investigating, mitigating the impact of or otherwise responding to the Data Breach, including by cooperating with Company for the purposes of Company notifying those affected by the Data Breach or any relevant regulator;

(viii) unless otherwise required by Law, not notify any third party of the effect of the Data Breach on Protected Data or on Company without Company's express prior consent. Where Contractor must by Law notify a third party, Contractor must, to the extent possible, consult with Company and allow Company to review and approve any notice before it is issued;

(ix) preserve and protect any affected Protected Data (including as necessary reverting to any backup or alternative site or take other action to recover Protected Data); and,

(x) promptly restore any lost or corrupt Protected Data using best practice data restoration techniques.

(f) Contractor must ensure all subcontracts and other supply chain arrangements, which may allow access to Protected Data, include protections for Protected Data which are consistent with this clause 5.

6. Trade Control Law compliance

Contractor:

(a) must, in performing its obligations under this Contract, comply with Trade Control Law;

(b) must not source and provide to Company any Goods, Work, or Services, or any component thereof, from any person, entity, or country, which is the target of Trade Control Law; and

(c) represents and warrants that it is not a Sanctioned Party and will not during the course of this Contract take any action(s) which cause it to become a Sanctioned Party. If Contractor so becomes a Sanctioned Party, it must notify Company as soon as possible.

7. Books, records, and audit right

(a) Contractor agrees it will:

(i) keep and maintain accurate and reasonably detailed books and financial records of expenses and receipts in connection with its performance under, and any payments made or received in connection with, this Contract (including any Purchase Order or SOW under it) for at least 8 years after the End Date; and

(ii) upon request promptly, and in any event no later than 7 days after such request, provide all such information (including Company Data, accounting books and financial records), assistance and cooperation as Company requires to audit,

investigate, or report on any matter in connection with, or related to Contractor's performance under, this Contract.

(b) Without limiting Company's rights under this clause 7, Company may at any time undertake, or engage a third party to undertake on its behalf, an audit of Contractor's (including any Contractor's Personnel's) compliance with any matter capable of being audited under this Contract.