Business Conduct Requirements

1. Definitions

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

Affiliate means, in respect of a Party or other entity, any corporation, company, partnership, limited partnership, limited liability company, joint venture or other form of business entity, which controls, is controlled by, or is under common control with, that Party or other entity.

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

Bribe means any offer of, payment of, or request for, directly or indirectly, any monetary or other thing of value to influence a Government Official or any other person to act improperly in performing his/her duties, including without limitation providing a facilitation payment, which is any payment or gift, even if small or low value, to a Government Official to speed up his/her performance of a routine and non-discretionary service or function.

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

Contractor means the counterparty to Company under the Contract.

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

Government Official includes any: 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); political party or party official, or political office candidate; and person acting on behalf of such government or public international organization, or any agency, department, or instrumentality.

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, including without limitation any permitted purpose categories of data listed in the Privacy Policy.

Personnel means directors, officers, employees, agents, or subcontractors (of any tier under a Party) of a Party and its Affiliates, and any director, officer, employee, agent, or invitee of any agent, invitee, subcontractor (of any tier under a Party) or Affiliate of a Party.

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

Process 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: any person or entity designated for export controls or sanctions restrictions under any Trade Control Law, including without limitation any applicable designation under United States (US) List of Specially Designated Nations and Blocked Persons, Foreign Terrorist Organization list, Specially Designated Global Terrorists list, Sectoral Sanctions Identification List, US Bureau of Industry and Security Entity List, United Kingdom Consolidated list, EU Consolidated List and Australia's Consolidated List; and/or 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, anti-money laundering, counter-terrorism financing or other regulations, orders, directives, designations, licenses or decisions

applicable to either Party or the Contract and relating to the trade or transfer of goods, technology, software and/or services which are imposed, administered or enforced from time to time, including but not limited to those established by Australia, the US, the United Kingdom, Singapore, the European Union (EU), EU Member States, or the United Nations.

2. Supplier Business Conduct. Contractor acknowledges it has access to, has read, and shall comply with the Code, Sustainability Policy, Privacy Policy, and Site Standards and Procedures, as applicable from time to time, and Contractor shall ensure all Contractor's Personnel read, understand, and will comply with, the same.

3. Anti-corruption Compliance

(a) Contractor represents, warrants, and undertakes:

(i) Contractor, and all Contractor's Personnel, shall comply with Anti-corruption Law;

(ii) Contractor and Contractor's Personnel has not and will not, directly or indirectly, give a Bribe to a Government Official or any person in order to obtain award of the Contract or while the Contract is effective;

(iii) Contractor shall promptly notify Company in writing, and in any event within 3 days, of receiving, directly or indirectly, any request or demand for any Bribe or payment of any kind (including, but not limited to, a ransom, facilitation or extortion payment), gift or other advantage that violates Anti-corruption Law in relation to Company or the Contract, regardless of whether Contractor agrees to such request or demand;

(iv) Contractor shall implement and maintain effective internal controls to prevent a breach of Anti-corruption Law by Contractor or Contractor's Personnel in connection with the Contract;

(v) all Contractor Personnel performing services under the Contract completed Anti-corruption Law training;

(vi) 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 the Contract;

(vii) 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;

(viii) if Contractor is to act, or may act, on Company's behalf (either directly or via a third party) in dealing with a Government Official when performing under the Contract, Contractor shall:

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

(B) perform appropriate anti-corruption due diligence on such third party, keep records of the same, and take reasonable measures to ensure such third party complies with clause 3 of these Requirements; and

(ix) it will notify Company in writing promptly upon becoming aware of any actual, suspected or imminent breach of clause 3 of these Requirements by Contractor or Contractor's Personnel.

(b) Nothing in this clause 3 prohibits Contractor or its Personnel from making payment or providing a service under extreme and imminent duress, if, and only if, such payment is absolutely necessary to preserve life, health, or physical safety of its Personnel, provided:

(i) such duress payments or services are permitted only if there is real and immediate threat to a person's life or liberty. Such payments or services are not permitted solely to preserve physical property or business opportunities; and

(ii) Contractor shall promptly, and in any event within 1 day, notify Company in writing of any duress payments made or services provided pursuant to this clause.

(c) Without limiting any rights of Company under Law, equity, or Contract, if Company reasonably suspects Contractor is in breach of or has breached clause 3, 4, 6 or 8 of these Requirements, or Company knows or reasonably suspects that such a breach is imminent, then:

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

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

4. Human Rights Compliance

(a) Contractor shall, and shall cause Contractor's Personnel to:

(i) not engage in any conduct which is 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 clause 4 of these Requirements at and in all of its operations and supply chains.

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

(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 shall notify Company in writing promptly upon, and in any event no later than 3 days after, becoming aware of any actual or potential breach of clause 4 of these Requirements.

5. Privacy and Data Security

(a) Contractor shall, 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 complaints 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 written 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: has custody or control over any of Company's Confidential Information; or 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 (collectively, "Company Data"), Contractor shall:

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

(ii) 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 to regularly verify and update these safeguards against risk(s) identified;

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

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

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

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

(vii) on termination or expiry of the Contract for whatever reason, 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

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

(c) Contractor shall 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 the 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 integrity, security, or confidentiality thereof, other than as directed by Company in writing.

(e) If Contractor becomes aware of any actual or suspected: misuse, interference, loss, or unauthorized Process, access, modification, or disclosure of Protected Data by any person; or breach of Contractor's obligations in relation to Protected Data; or 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 shall (at its own cost):

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

(ii) mitigate any harmful effect of the Data Breach;

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

(iv) provide any assistance requested by Company for the 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;

(v) 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 written consent. Where Contractor must by Law notify a third party, Contractor shall consult with Company and allow Company to review and approve any notice before it is issued;

(vi) 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

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

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

6. Trade Control Law

(a) Contractor shall, and shall cause Contractor's Personnel to:

(i) in performing its obligations under the Contract, comply with Trade Control Law;

(ii) not, in performing its obligations under the Contract, engage in or attempt to engage in any financial transaction involving, or otherwise deal in, funds which Contractor knows or reasonably suspects may represent the proceeds of a crime in violation of Trade Control Law;

(iii) not, in performing its obligations under the Contract, physically transport or attempt to physically transport monetary instruments or funds which Contractor knows or reasonably suspects may represent the proceeds of a crime or for the purpose of carrying on a crime in violation of Trade Control Law;

(iv) not, in performing its obligations under the Contract, provide any payment (including, but not limited to, ransom, toll, safe passage, or extortion payments) or service to, or request any payment or service from, a Sanctioned Party in violation of Trade Control Law; and

(v) not source and provide to Company any goods or services, or any component thereof, from or involving: any Sanctioned Party; or any person, entity or country, which is otherwise the target of Trade Control Law.

(b) Contractor represents, warrants, and undertakes:

(i) it will notify Company in writing promptly, and in any event within 3 days, of any payment, provision of services, or request or demand for any payment or service that violates Trade Control Law or which Contractor reasonably suspects may violate Trade Control Law in relation to Company or the Contract;

(ii) it will notify Company in writing promptly, and in any event within 3 days, of any irregular or unusual request for payment or services (such as requests for ransom, toll, safe passage, or extortion payments), even where Contractor does not know or reasonably suspect such payment or service may violate Trade Control Law in relation to Company or the Contract;

(iii) it will implement and maintain effective internal controls to prevent a breach of Trade Control Law in connection with the Contract;

(iv) all Contractor Personnel performing services under the Contract have completed Trade Control Law compliance training; and

(v) it is not a Sanctioned Party and will not during the course of the Contract take any action which cause it to become a Sanctioned Party. If Contractor becomes, or reasonably suspects it will become, a Sanctioned Party, it shall notify Company in writing immediately.

(c) Without limiting any rights of Company under Law, equity, or Contract, if Company reasonably suspects Contractor is in breach of or has breached clause 6 of these Requirements, or Company knows or reasonably suspects that such a breach is imminent, then:

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

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

7. Books, records and audit rights

(a) Contractor shall:

(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, the Contract (including any Purchase Order or SOW under it) for at least 10 years after the End Date;

(ii) implement and maintain at all times appropriate internal controls to ensure any payments made in connection with the Contract (including any Purchase Order or SOW under it) are properly, accurately, and completely recorded; and

(iii) 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), access to Contractor's Personnel, assistance and cooperation to Company as Company requires to monitor, audit, investigate or report on any matter in connection with, or related to Contractor's performance under, the Contract. Company has the right to make and retain copies of any such documents or records.

(b) Without limiting Company's rights under this clause 7 of these Requirements, 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 the Contract.

8. Customs Trade Partnership Against Terrorism (CTPAT) Compliance

(a) Contractor shall maintain, and where required shall obtain, all Customs Trade Partnership Against Terrorism ("CTPAT") certifications, validations and approvals necessary for Contractor's performance under the Contract.

(b) Contractor shall:

(i) implement and maintain processes to verify, monitor and document its ongoing compliance with applicable CTPAT Minimum Security Criteria, as amended from time to time;

(ii) promptly notify Company of any actual or suspected non-compliance with CTPAT requirements, and any suspension, lapse, revocation, or adverse change in the CTPAT status of Contractor, and promptly implement corrective actions to address any identified deficiencies; and

(iii) maintain records demonstrating compliance with this clause and make such records available to Company upon request.