# RIO TINTO CYBER SECURITY REQUIREMENTS FOR SUPPLIERS

Suppliers must ensure their information technology and other business systems meet the following requirements when providing their Supply to the Rio Tinto group of companies or otherwise interfacing with Rio Tinto's enterprise and industrial and operational technology systems.

## 1. GENERAL

(a) Any technology systems utilised or services provided by the Supplier, or significant modification of an existing system or services, must not expose Rio Tinto to material cybersecurity risk.

(b) Supplier must ensure it has conducted an appropriate cyber security risk assessment on its own systems (and any third party systems) utilised in providing the Supply, in particular:

(i) identify the key technical, and compliance measures required to ensure the confidentiality, integrity and availability of information is maintained; and

(ii) ensure that control measures applied are commensurate with assessed risk.

The results of any risk assessment will be made available to Rio Tinto on request.

(c) Key technology systems operated by the Supplier have response and recovery plans, with recovery plan testing being undertaken periodically to ensure procedures and controls are effective and services are able to be restored as soon as possible.

(d) On termination of a relationship between Rio Tinto and the Supplier, Supplier must ensure the following (including as applicable to any third party systems utilised by the Supplier):

(i) the return, or the destruction, of Rio Tinto information held by the Supplier;

(ii) any access to the Rio Tinto environment is terminated, and

(iii) any Rio Tinto intellectual property appropriately transitioned back to Rio Tinto.

## 2. ACCESS CONTROLS

To the extent the Supplier requires access to any Rio Tinto information technology or business systems as part of the Supply, the Supplier must ensure the following:

(a) access to any Rio Tinto systems must be appropriately restricted to only the Supplier personnel requiring access to complete the Supply;

(b) access procedures must cover identification, authentication, authorisation and auditing requirements;

(c) each user identity requiring access to Rio Tinto systems is linked to or owned by a uniquely identifiable individual;

(d) users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction;

(e) where access is required from outside the Rio Tinto network, multi factor authentication must be used for client access; and

(f) information related to, or generated by, account management activities must be documented and retained for auditing purposes;

## 3. REMOTE ACCESS TO RIO TINTO SYSTEMS

To the extent Supplier or its personnel requires access to Supplier's information technology or business systems located within Rio Tinto's network environment provided as part of the Supply, the Supplier must ensure the following:

(a) remote access is securely designed and managed;

(b) access is provided only to authorised parties for valid business reasons;

(c) access is revoked where no longer required;

(d) it will follow the required minimum technical controls to support the secure operation of remote access as specified by Rio Tinto; and

(e) it will periodically review and monitor such remove access when no longer required.

## 4. NETWORK INTEGRITY

When accessing Rio Tinto's information technology network, Supplier must do all things reasonably required to ensure that Rio Tinto's network integrity remains protected, including:

(a) maintaining effective Network Segregation and Network Segmentation. Network Segregation and Network Segmentation must be implemented at the gateway between network zones and achieved by enforcing rulesets to control and filter communications between network zones; and

(b) employing a "deny by default" approach, with rules that permit communications across zones being IP source, IP destination and TCP/UDP port specific. Any rules that permit either all source IP addresses, destination IP addresses, or any type of service/protocol must not be used.

For the purpose of this clause:

"**Network Segregation**" means to "segregate" a network from other networks with a differing level of trust.

"**Network Segmentation**" means to "segment" a network into smaller network segments or zones, based on factors such as management authority, level of trust, functional criticality, and amount of communications traffic required to cross-zone boundaries.

## 5. INFORMATION PROTECTION

The Supplier must ensure the following to the extent it applies to the Supply to Rio Tinto:

(a) Establish and maintain effective change control processes including:

(i) determining the types of changes to the Supplier's information system that are configuration-controlled with explicit consideration for security impact analyses;

(ii) documenting configuration change decisions associated with the Supplier's information system

(iii) complying with Rio Tinto's applicable change management processes; and

(iv) retaining adequate records of configuration-controlled changes to the Supplier's information system to be provided to Rio Tinto on request;

(b) Maintain response and recovery plans incorporating the following:

(i) Disaster Recovery Plans (DRPs) for critical systems, incorporating essential service continuity, response and recovery requirements for these systems, and taking into consideration relevant cybersecurity threats and scenarios.

(ii) DRP testing on a periodic basis to ensure procedures and controls are effective, and services restored are able to be restored within required as soon as possible.

## 6. DATA SECURITY

The Supplier must ensure appropriate encryption standards are applied to Rio Tinto information, including:

(a) information classified by Rio Tinto as 'Confidential' or 'Highly Confidential' when Stored At Rest by the Supplier;

(b) information exchanged through the internet, irrespective of its classification.

For the purpose of this clause:

"**Stored At Rest"** means information stored by the Supplier on Removable Media or backup media stored by the Supplier at off-site premises.

## 7. REMOVABLE MEDIA

The Supplier must ensure the following:

(a) that all Removable Media is protected and its use restricted only to those Supplier personnel requiring such access as part of the Supply;

(b) maintain documented procedures for the management of Removable Media, including the specification of approved media, processes of handling and disposal, as well as the technical enforcement of controls; and

(c) comply with any security controls for Removable Media reasonably required by Rio Tinto and provide details of such compliance to Rio Tinto on request.

For the purpose of this clause:

"**Removable Media**" means computers storage devices designed to be inserted and removed from a computer/system, including but not limited to optical discs and USB flash drivers