RioTinto

RIO TINTO CYBER SECURITY REQUIREMENTS FOR SUPPLIERS

All suppliers must ensure that any information technology and other business systems used to deliver their Supply to the Rio Tinto Group, or any systems that interact with Rio Tinto Group's Information Technology (IT) or Industrial and Operational Technology (I&OT) systems, comply with the following cyber security requirements.

1. GENERAL

The Supplier must ensure that any technology systems it utilises or any services it provides, along with any significant modification to existing systems or services, do not expose Rio Tinto to material cyber security risk. Rio Tinto shall have sole discretion in determining what constitutes a material risk.

2. CYBER SECURITY RISK ASSESSMENT

The Supplier must conduct, document and provide, upon request, to Rio Tinto a cyber security risk assessment. This assessment must:

(a) Cover the Supplier's systems and any third-party systems involved in providing the Supply.
(b) Identify the key technical and compliance measures required to maintain the confidentiality, integrity, and availability of information.
(c) Ensure that control measures applied are proportionate to the level of risk identified.

This requirement may not apply if the Supplier provides current and relevant cyber security governance attestations—such as ISO/IEC 27001 certification or a SSAE18/ISAE3402 SOC 2 Type II report—issued by a suitably qualified and independent third party covering the relevant systems used in the Supply. Rio Tinto reserves the right to request additional evidence or third-party attestation at its discretion.

3. ACCESS CONTROL

3.1 ACCESS TO RIO TINTO'S ASSETS

Where the Supplier requires access to any of Rio Tinto's technology systems as part of the Supply, the Supplier must ensure that:

(a) Access is provisioned by Rio Tinto through Rio Tinto's identity provider.
(b) Access is strictly limited to the Supplier personnel who require it to perform their duties related to the Supply.
(c) Access is limited to the period required for service delivery. The Supplier must promptly notify Rio Tinto when access is no longer required so it can be revoked, even if the original access period has not yet expired.
(d) Each user identity that is provisioned with access is uniquely linked to an identifiable individual.
(e) All users, devices, and other identities are authenticated into Rio Tinto's network using multifactor authentication (MFA).

3.2 REMOTE ACCESS TO THE SUPPLIER'S ASSETS LOCATED IN RIO TINTO'S NETWORK

Where the Supplier requires access to its own technology systems provided as part of the Supply, and these systems reside within Rio Tinto's network environment, the Supplier must ensure that:

(a) All remote access solutions used to access Rio Tinto's networks are pre-approved and managed by Rio Tinto.
(b) Access is granted only to authorised individuals and solely for legitimate business purposes.
(c) Access is continuously monitored, periodically reviewed, and promptly revoked when no longer required.
(d) The minimum technical controls required to support the secure operation of remote access, as specified by Rio Tinto, are consistently met and maintained.

4. NETWORK SECURITY

When accessing Rio Tinto's networks, the Supplier must take all reasonable measures to ensure that Rio Tinto's network security is not compromised, including:

(a) Ensuring that the Supplier's own networks are effectively segregated from Rio Tinto's networks.
(b) Enforcing rulesets at the gateway between network zones to control and filter traffic ensuring effective segregation and segmentation[1]. The gateway must be pre-approved and managed by Rio Tinto.
(c) Adopt a "deny by default" rule approach, allowing only explicitly defined traffic between zones. Permit rules must specify IP source, IP destination, and TCP/UDP port, and must not use "ANY" for sources, destinations, or services/protocols.

5. SERVICE RESILIENCE AND DISASTER RECOVERY PLAN

5.1 The Supplier must ensure the availability and resilience of its key technology systems and data used to deliver the Supply, such that the Supply to Rio Tinto can be restored as quickly as practicable in the event of an outage. While the specific measures implemented by the Supplier (e.g., use of availability zones, periodically tested response and recovery plans, backup restoration procedures, etc.) may vary, they must provide clear and demonstrable assurance that the Supply can be restored within an acceptable timeframe.

5.2 The Supplier must maintain Disaster Recovery Plans (DRPs) for all its critical systems for the duration that Services are provided to Rio Tinto and for as long as the Supplier's name or brand remain publicly associated with Rio Tinto, regardless of whether Services are currently being delivered. These obligations apply in addition to any service-specific DRP requirements set out elsewhere. All DRPs must:

i. Address essential service continuity, including response and recovery requirements.
ii. Consider relevant cyber security threats and scenarios.
iii. Be tested on a periodic basis to ensure that procedures and controls are effective, and that systems and services can be restored within acceptable timeframes.

6. CHANGE MANAGEMENT

6.1 Where applicable to the Supply provided to Rio Tinto, the Supplier must establish and maintain effective change control processes. These processes must:

(a) Comply with Rio Tinto's applicable change management processes.
(b) When identifying the types of changes to the Supplier's systems that require configuration control,

[1] For the purposes of this clause, "network segregation" refers to the practice of isolating one network from other networks with different levels of trust, and "network segmentation" refers to dividing a network into smaller segments or zones based on factors such as management authority, level of trust, functional criticality, and the volume of data traffic that must traverse zone boundaries.

explicitly evaluate their potential security impact.
(c) Document all decisions associated with configuration change made to the Supplier's systems.
(d) Retain detailed records of all configuration-controlled changes made to the Supplier's systems.

6.2 Upon request, the Supplier must provide Rio Tinto with access to records of configuration-controlled changes related to the systems used in delivering the Supply.

7. ENCRYPTION

The Supplier must ensure that strong encryption is applied to Rio Tinto's information in line with industry best practices (e.g., NIST FIPS and SP 800 series, ISO/IEC standards), including:

(a) All information classified by Rio Tinto as 'Confidential' or 'Highly Confidential' when stored at rest[2] in the Supplier's systems, and within transit.
(b) All information, irrespective of its classification, when transmitted over the internet (i.e., in transit).

8. REMOVABLE MEDIA

8.1 Removable media[3] must not be connected to any Rio Tinto electronic device unless prior written approval has been obtained from Rio Tinto Cyber Security.
8.2 Where use of removable media is approved by Cyber Security, the Supplier must:
(a) Restrict access to removable media to only those Supplier personnel who require it to perform their duties in connection with the Supply.
(b) Ensure that all removable media is protected at all times and free of malware.
(c) Maintain documented procedures for the secure management of removable media. These procedures must:
i. Define approved media types.
ii. Outline secure handling and disposal processes.
iii. Describe the technical controls used to enforce these requirements.
iv. Be made available to Rio Tinto upon written request.

9. TERMINATION OF THE RELATIONSHIP

Upon termination of the relationship between Rio Tinto and the Supplier, the Supplier must ensure that:

(a) All Rio Tinto's information held by the Supplier, both in its own systems and in any third-party system it utilises, is either returned to Rio Tinto in a standard format
(b) or securely destroyed, in accordance with Rio Tinto's instructions.
(c) All access to Rio Tinto's environments from the Supplier's side (if any), including any access granted to personnel and third parties, is immediately terminated. The Supplier must certify in writing to Rio Tinto that such access has been revoked.
(d) Any Rio Tinto's intellectual property is immediately transitioned back to Rio Tinto.

[2] For the purposes of this clause, "stored at rest" means information stored by the Supplier on removable media or backup media at off-site premises.
[3] For the purposes of this clause, "removable media" refers to portable storage devices designed to be inserted into and removed from a computer or system, including, but not limited to, optical discs and USB flash drivers.