METALS ACQUISITION LTD

Information Security Policy
As of August 23, 2023

1.0 PURPOSE

This Information Security Policy (the "Policy") defines, documents, and supports the implementation and maintenance of the administrative, technical, and physical safeguards that Metals Acquisition Limited ("MAC") has selected to protect the personal information that it collects, creates, uses, and maintains. This Policy has been developed in accordance with industry guidelines, relevant regulations, and applicable law. If this Policy conflicts with any legal obligation or other MAC policy or procedure, the provisions of this Policy shall govern unless the General Counsel specifically reviews, approves, and documents an exception in accordance with Section 3.4 of this Policy.

The specific purposes of this Policy are to:

1.1. Ensure the security, confidentiality, integrity, and availability of the personal information that MAC collects, creates, uses, and maintains.

1.2. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

1.3. Protect against unauthorized access to or use of MAC-maintained personal information that could result in substantial harm or inconvenience to any customer or employee.

1.4. Define an information security program that is appropriate to MAC's size, scope, and business, its available resources, and the amount of personal information that MAC owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

2.0 SCOPE

This policy applies to all MAC personnel (including its employees, consultants, and contractors). It applies to any records that contain personal information in any format and on any media, whether in electronic or paper form.

3.0 RESPONSIBILITIES

The Nominating and Corporate Governance Committee–has designated the General Counsel to implement, coordinate, and maintain this Policy. The General Counsel shall be accountable for:

3.1. Initial implementation of this Policy, including:

3.1.1. Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 5.0);

3.1.2. Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 6.0);

3.1.3. Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information (see Section 7.0);

3.1.4. Ensuring that the safeguards are implemented and maintained to protect personal information throughout MAC, where applicable (see Section 7.0);

3.1.5. Overseeing service providers that access or maintain personal information on behalf of MAC (see Section 8.0);

3.1.6. Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 9.0);

3.1.7. Defining and managing incident response procedures (see Section 10.0); and

3.1.8. Establishing and managing enforcement policies and procedures for this Policy, in collaboration with MAC human resources and management (see Section 11.0).

3.2. Employee, contractor, and (as applicable) stakeholder training, including:

3.2.1. Providing periodic training regarding this Policy, MAC's safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal information;

3.2.2. Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through written acknowledgement forms; and,

3.2.3. Retaining training and acknowledgment records.

3.3. Reviewing this Policy and the security measures defined by this Policy at least annually, or whenever there is a material change in MAC's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information (see Section 12.0).

3.4. Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this Policy or MAC's information security policies and procedures.

3.5. Periodically reporting to MAC management regarding the status of the information security program and MAC's safeguards to protect personal information.

MAC recognizes that the General Counsel is a key role and accountable for significant requirements. MAC shall commit the necessary resources, budget, authority, and access to executive management to this role.

4.0 DEFINITIONS

4.1. **Personal Information –** has the meaning given to that term within laws relating to privacy and data security, including the *Privacy Act 1988* (Cth) (the **Privacy Act**), applicable to MAC (**Privacy Laws**) whether such Privacy Laws use the term "personal information", or a substantially similar term (such as 'personal data' or 'personally identifying information'), and for the purposes of this policy includes:

4.1.1. **General Personal Information** – being any information or opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether recorded in a material form or not;

4.1.2. Sensitive Information – being any General Personal Information that includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation, criminal record, health information (including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional that is created, received, or otherwise stored by MAC) (**Health Information**) and genetic or biometric information (including biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris) (**Biometric Information**); and

4.1.3. **Personally Identifying Information** – being General Personal Information that specifically includes an individual's first and last name or first initial and last name in combination with one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could reasonably be used to identify an individual or to commit identity theft:

4.1.3.1. Social Security number, Tax File Number;

4.1.3.2. Driver's license number, other government-issued identification number, including passport number, or tribal identification number;

4.1.3.3. Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial account;

4.1.3.4. Health Information,;

4.1.3.5. Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer;

4.1.3.6. Biometric Information; or,

4.1.3.7. Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

5.0 RISK ASSESSMENT

As a part of developing and implementing this Policy, MAC will conduct a periodic, documented risk assessment, at least annually, or whenever there is a material change in MAC's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal information.

5.1. The risk assessment shall:

5.1.1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal information;

5.1.2. Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal information; and

5.1.3. Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

5.1.3.1. Employee, contractor, and (as applicable) stakeholder training and management;

5.1.3.2. Employee, contractor, and (as applicable) stakeholder compliance with this Policy and related policies and procedures;

5.1.3.3. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

5.1.3.4. MAC's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

5.2. Following each risk assessment, MAC will:

5.2.1. Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;

5.2.2. Reasonably and appropriately address any identified gaps; and

5.2.3. Regularly monitor the effectiveness of MAC's safeguards, as specified in this Policy (see Section 7.0).

6.0 INFORMATION SECURITY POLICIES AND PROCEDURES

As part of this Policy, MAC will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders to:

6.1. Establish policies regarding:

6.1.1. Information classification;

6.1.2. Information handling practices for personal and other sensitive information, including the storage, access, disposal, and external transfer or transportation of personal and other sensitive information;

6.1.3. User access management, including identification and authentication (using passwords or other appropriate means);

6.1.4. Encryption;

6.1.5. Computer and network security;

6.1.6. Physical security;

6.1.7. Incident reporting and response;

6.1.8. Employee and contractor use of technology, including Acceptable Use and Bring Your Own Device to Work (BYOD); and

6.1.9. Information systems acquisition, development, operations, and maintenance.

6.2. Detail the implementation and maintenance of MAC's administrative, technical, and physical safeguards (see Section 7.0).

7.0 SAFEGUARDS

MAC will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal information that MAC owns or maintains on behalf of others in accordance with the following:

7.1. Safeguards shall be appropriate to MAC's size, scope, and business, its available resources, and the amount of personal information that MAC owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

7.2. MAC shall document its administrative, technical, and physical safeguards in MAC's information security policies and procedures (see Section 6.0).

7.3. MAC's administrative safeguards shall include, at a minimum:

7.3.1. Designating one or more employees to coordinate the information security program (see Section 3.0);

7.3.2. Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 5.0);

7.3.3. Training employees in security program practices and procedures, with management oversight (see Section 3.1.8);

7.3.4. Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 8.0); and

7.3.5. Adjusting the information security program in light of business changes or new circumstances (see Section 12.0).

7.4. MAC's technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

7.4.1. Secure user authentication protocols, including:

7.4.1.1. Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;

7.4.1.2. Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records; and

7.4.1.3. Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

7.4.2. Secure access control measures, including:

7.4.2.1. Restricting access to records and files containing personal information to those with a need to know to perform their duties; and

7.4.2.2. Requiring each individual with computer or network access to use unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.

7.4.3. Encryption of all personal information traveling wirelessly or across public networks;

7.4.4. Encryption of all personal information stored on laptops or other portable or mobile devices, and to the extent technically feasible, personal information stored on any other device or media (data-at-rest);

7.4.5. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal information or other attacks or system failures;

7.4.6. Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal information; and

7.4.7. Reasonably current system security software (or a version that can still be supported with reasonably current patches and malicious software definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

7.5. MAC's physical safeguards shall, at a minimum, provide for:

7.5.1. Defining and implementing reasonable physical security measures to protect areas where personal information may be accessed, including reasonably restricting physical access and storing records containing personal information in locked facilities, areas, or containers;

7.5.2. Preventing, detecting, and responding to intrusions or unauthorized access to personal information, including during or after data collection, transportation, or disposal; and

7.5.3. Secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

8.0 SERVICE PROVIDER OVERSIGHT

MAC will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal information on its behalf by:

8.1. Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this Policy and all applicable laws and MAC's obligations.

8.2. Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this Policy and all applicable laws and MAC's obligations.

8.3. Monitoring and auditing the service provider's performance to verify compliance with this Policy and all applicable laws and MAC's obligations.

9.0 MONITORING

MAC will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal information. MAC shall reasonably and appropriately address any identified gaps.

10.0 INCIDENT RESPONSE

MAC will establish and maintain policies and procedures regarding information security incident response (see Section 6.1.7). Such procedures shall include:

10.1. Documenting the response to any security incident or event that involves a breach of security.

10.2. Performing a post-incident review of events and actions taken.

10.3. Reasonably and appropriately addressing any identified gaps.

11.0 ENFORCEMENT

Violations of this Policy will result in disciplinary action, in accordance with MAC's information security policies and procedures and human resources policies. Please applicable HR policies for details regarding MAC's disciplinary process.

12.0 PROGRAM REVIEW

MAC will review this Policy and the security measures defined herein at least annually, or whenever there is a material change in MAC's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information.

MAC shall retain documentation regarding any such program review, including any identified gaps and action plans.

13.0 EFFECTIVE DATE

This Policy is effective as of the date shown in the document header. Revision and review history for this Policy can be found in Appendix A.

Appendix A - Revision and Review History

Intentionally blank as at effective date