LithiumArgentina

IT and Cybersecurity Policy

January 2025

I. Purpose and Scope

This is the Information Technology ("**IT**") and Cybersecurity policy (the "**Policy**") of Lithium Argentina AG ("**Lithium Argentina**" or the "**Company**"), which outlines the Company's requirements for preserving the security of our data and technology infrastructure. It applies to all Executive Management, Officers and Workforce who use or have permanent or temporary access to the Company's information technology systems or hardware. The term "Company" shall include Lithium Argentina's subsidiaries unless the context dictates otherwise.

1. General

The Company relies on technology to collect, store, and manage information and therefore we are vulnerable to security breaches. Human error, attacks by hackers and system malfunctions can cause a high level of financial damage to the Company and jeopardize the Company's reputation. This Policy provides the minimum requirements to ensure the security of the Company's confidential information, technology assets, and intellectual property are protected.

Questions regarding this Policy can be directed to the IT Department for your office, as set out in the contact sheet on the Company's intranet.

2. Application to Minera Exar S.A.

This Policy has also been adopted by Minera Exar S.A. ("**Minera Exar**") as a policy of Minera Exar applicable to all of its employees, directors, officers, and consultants. Minera Exar embraces the principles this Policy and will enforce it as part of its policies and procedures. Lithium Argentina shall have no responsibility or liability to enforce this Policy insofar as it applies to Minera Exar. Unless otherwise specified, references to the "Company", "we", "our", or "us" in the definitions below and in other sections of this Policy shall refer to Minera Exar and its subsidiaries in so far as it relates to the application of this Policy to Minera Exar and/or its subsidiaries, their business and operations and their employees, directors, officers and consultants. Minera Exar may adopt additional policies and procedures for the implementation and administration of this Policy.

II. Confidential Data

Confidential data is secret and valuable. Confidential data applies to sensitive business information which unauthorized modification or disclosure of could adversely impact the Company, its shareholders,

business partners, or customers. This information should be protected/restricted. Disclosure thereof requires the appropriate approval and in the case of third parties, a signed confidentiality and non-disclosure agreement.

Common examples include:

- Unpublished financial information.
- Data suppliers, vendors, partners, and customers.
- Patents, formulas or new technologies.
- Customer lists (existing and prospective).
- Legal agreements.
- Emails and attachments that include any confidential information, such as the above.

III. Definitions

"**Board**" means the Board of Directors of the Company.

"**Director**" means a member of the Board.

"**Executive Management**" means the Executive Chairman, the Chief Executive Officer ("**CEO**"), Chief Financial Officer ("**CFO**") and the Executive Vice President, Corporate Development.

"**Officer**" means an individual appointed by the Board or CEO as an officer in accordance with the Company's Articles of Association.

"**Workforce**" means all employees of the Company and its subsidiaries, and consultants and anyone working at a Company project, operation, or office.

IV. Protect Personal and Company Devices

When you use a digital device, such as a cell phone or laptop, to access Company emails or accounts, you introduce security risk to the Company's data. We advise you to keep your personal and Company-issued computers, tablets, and cell phones secure. You can maintain security by:

- Keeping all devices password protected. Choose strong passwords and store passwords in a secure location. Password requirements with respect to minimum length and complexity as well as automatic lock-out for failed attempts are set by the IT Department.
- Implementing multi-factor authentication ("**MFA**") on Company and personal devices. Multi-factor authentication must always be required if access to the Company's network is requested from non-Company devices and is enforced centrally by the IT Department.
- Ensuring you do not leave any devices unattended or within view of others while accessing confidential or sensitive Company information.
- Logging into Company accounts and systems through secure and private networks only and using VPN while travelling to secure and encrypt communications. It is recommended that you turn off the automatic connection to public networks on any personal devices you use to access Company information, including Company email.

Please do not access internal systems and accounts from other people's devices or lend your personal devices to others if the devices provide access to Company information.

If you are a new hire receiving Company-issued equipment, you will receive your equipment with the following security features pre-installed by the IT Department:

- Antivirus/ anti-malware software.
- Login password set-up.
- Access and password protection to the Company VPN networks.
- Instructions on accessing internal software or network data storage.
- Multi-factor authentication.

You should follow the instructions to protect physical devices and refer to the Company's IT Department if you have any questions.

V. Keep Emails Safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, employees should:

- Avoid opening attachments and clicking on links when the content is not adequately explained or not from a trusted source (e.g. "watch this video, it's amazing.").
- Be suspicious of clickbait titles (emails promoting prizes, gifts, advice etc. with the main purpose to attract attention and encourage visitors to click on a link).
- Be alert to "Spoofing" email, which are email messages with a forged sender address. Check email and names of people you received a message from to ensure the message is legitimate. Check the properties of the sender in the email to check if the email address is legitimate. Or click reply without sending to see if the same email address appears in the reply email, then delete the reply message without sending if the recipient email address is unfamiliar to you or appears to be a different reply address than appearing in the properties of the sender.
- Be alert for inconsistencies or giveaways (e.g. grammar mistakes, non-typical style of emails, capital letters and excessive number of exclamation marks.

The following restrictions apply to use of the Company email:

- Conducting or running a personal business via Company email.
- Any illegal activity, including but not limited to, mail fraud, slander, harassment, or any other activity that violates local, provincial, state, or federal law.
- Sending documents or copying materials in violation of copyright laws.
- Attempting to breach security measures, intercept email communications, or gain unauthorized access to any email system.
- Using Company email to solicit or recruit others for commercial purposes, outside organizations, or non-job related purposes.
- Sending electronic greeting cards or mass mailing not related to company business.
- Forwarding personal messages containing comments or statements that may be mistaken as the position of the Company.
- Disclosing confidential Company information without appropriate approval.
- Sending unsolicited email messages, including sending junk mail, chain letters or any other advertising material to individuals who did not specifically request it (emailing spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of message.
- Unauthorized use or forging of an email header (used to identify sender's details).
- Solicitation of email for any other email address, other than that of the user's account, with the intent to harass or collect replies.

Email is a useful tool for communication with internal and external stakeholders. Emailed information

can be easily and readily distributed. Employees should consider if it is better to share information using other methods for working copies to comply with information security.

If an employee isn't sure that an email they received is safe, they can refer to our IT Department.

VI. Manage Passwords Properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to align their password with the Company's password policy:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g. birthdays). A policy with respect to the length and complexity of passwords is centrally enforced by the IT Department with pre-installed IT configuration.
- Remember passwords instead of writing them down whenever possible. Use an encrypted password manager tool to generate and securely store passwords.
- Do not exchange credentials with other employees and do not provide your credentials to anybody.

VII. Transfer Data Securely

Transferring data introduces security risk. Employees must:

- Before transferring sensitive data to vendors or elsewhere external to the Company network, obtain the necessary approval from a supervisor, if applicable, arrange encryption of data by the IT Department and ensure that there is a confidentiality and non-disclosure agreement in place with the receiving party that requires them to protect the confidential nature of information being transferred.
- Not transfer sensitive data (i.e.: Company information etc.) to personal devices or accounts.
- Share confidential data over the Company network/system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate IT security policies.
- Report scams, privacy breaches, and hacking attempts to the IT Department

VIII. Reporting

Our IT Department needs to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, you must report all perceived attacks, suspicious emails, or phishing attempts as soon as possible to our IT Department. Our IT Department will investigate promptly, resolve the issue, and send a companywide alert when necessary.

Our IT Department can provide assistance to you on how to detect scam emails. We encourage you to reach out to them with any questions or concerns.

Please avoid overloading the IT Department with every spam email you receive. If you would like the IT Department to block spam emails, please attempt to consolidate such emails in one message to improve efficiency of communication.

IX. Additional Security Measures

To reduce the likelihood of security breaches, we ask you to:

- Lock your devices when leaving your desk by pressing the CTRL, ALT, and DEL keys and choosing “lock”.
- Report stolen or damaged equipment as soon as possible to the IT Department.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in Company systems to the IT Department.
- Consult with the IT Department before installing any software on your computers to ensure that the software is licensed and legitimate. Under no circumstances install unlicensed, pirated, suspicious, or illegal software (including but not limited to games (especially free games), “coupon finders”, driver installers, “Clean My PC” type applications, and other non-Company-provided software).
- Avoid accessing suspicious websites.

Our IT Department perform the following security activities:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange security training for employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy, as others do.
- Install updates to critical software after appropriate testing, including a plan to transition between major updates to avoid interruptions to critical business functions.

X. Remote Employees

If you are working remotely, you must also adhere to this policy. This is because you will be accessing our Company’s accounts and systems from a distance; as such, you are required to follow all data encryption and protection requirements of this policy to ensure your private network is secure.

We encourage you to seek advice from the Company’s IT Department and discuss local legal requirements or limitations for jurisdictions where security software is governed by regulations.

The Company reserves the right to monitor all devices and systems (including files saved and database, email, internet and systems activity) both for maintenance and security purposes. As such, you should not expect privacy when using any Company device or system. The Company owns everything stored or created on a Company device or system.

XI. Use of Company Devices and Systems

Company devices and systems, including software and internet services, are provided for business use. We understand that you may wish to use Company devices and systems for personal use. Such use should be occasional, not result in any additional expense to the Company and be for personal purposes that are consistent with our Code of Business Conduct and Ethics. When using Company devices or systems for personal use, you must never:

- Create email, online content, or other material that attribute your personal opinions to the Company.

- Break the law, including copyright laws, and human rights laws.
- Access, create or store inappropriate content (i.e.: pornography or gambling).
- Operate a personal business, unless you are using our systems and devices to provide services to the Company as an external contractor.
- Modify or disable system or security settings.
- Distribute religious, political, commercial, spam, or chain messages.
- Impersonate someone, including using co-workers devices, accounts, or passwords.

XII. Return Broken Devices

Broken and obsolete devices, including laptops, tablets, USB drives, peripheries, and Company-supplied smart phones should be returned to the IT Department.

XIII. Communication and Non-Compliance

If you are new to the Company, you will be provided with a copy of this Policy and can contact your supervisor, the IT Department, Human Resources, or the Corporate Secretary of the Company (and the applicable equivalent at Minera Exar) if you have any questions. This Policy will be circulated Company-wide whenever any changes are made.

Any breach of this Policy or failure to comply with its requirements could result in disciplinary action being taken by the Company, up to and including termination of employment or the contractual relationship. We will examine each incident on a case-by-case basis.

The key takeaway is that we ask everyone at the Company to take cybersecurity seriously. Everyone, from our employees, partners and customers, as well as our contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect Company systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

XIV. Amendments

This Policy will be reviewed periodically as determined necessary by Executive Management and submitted to the Board for its approval. Any minor changes that do not impact the objectives of the Policy may be updated by Management as necessary.

Approved by: Board of Lithium Argentina effective January 23, 2025