Information Technology Policy

SYRAH RESOURCES

www.syrahresources.com.au

enquiries@syrahresources.com.au

03 9670 7264

CONTENTS

1. INTRODUCTION

Syrah Resources Limited ("Syrah" or "the Company") is an Australian Securities Exchange listed industrial minerals and technology company with its flagship Balama Graphite Operation in Mozambique and a downstream Active Anode Material Facility in the United States. Syrah's vision is to be the world's leading supplier of superior quality graphite and anode material products, working closely with customers and the supply chain to add value in battery and industrial markets.

2. PURPOSE

The purpose of this Policy is to define clear and consistent standards of appropriate Information Technology ("IT") usage within the Syrah Group, ensuring that all employees understand their responsibilities in maintaining the confidentiality, integrity, and availability of company data and IT resources and to confirm the responsibilities of employees in relation to IT usage.

This Policy provides guidelines for the appropriate use of work devices, personal devices on Company networks and the escalation process for IT-related issues.

By setting these standards, the Policy aims to protect the employee and the Company from risks, including virus attacks, compromise of network systems and services, security breaches, unauthorized access and legal liabilities.

3. SCOPE

This Information Technology Policy ("Policy") applies to all Syrah Group employees, contractors, consultants, temporary workers and representatives of the Syrah Group, herein referred to as "Employee(s)".

The Syrah Group means Syrah Resources Limited and all related subsidiaries, including Twigg Exploration & Mining Limitada, Syrah Resources & Trading DMCC, Syrah Global DMCC and Syrah Technologies LLC. A reference in this Policy to "Syrah" or the "Company" includes each member of the Syrah Group.

This Policy also applies to contractors and third-party representatives who require access to IT resources to carry out their role in the business, including, but not limited to software and hardware vendor support personnel. These third parties are required to adhere to this Policy to ensure the protection and proper management of the Company's IT resources and data.

For the purpose of this Policy, "IT resource" or "IT asset" is the property of the Company and refers to any computer equipment, network resource or accounts providing electronic mail, internet, intranet, Wi-Fi, mobile device, software, operating systems, storage media, or any other IT equipment provided by the Company for Employees to carry out their job functions, for business purposes in serving the interests of the Company. Personal IT resources that are used for work purposes are also included within the scope of this Policy.

4. POLICY COMPLIANCE AND BREACH

Employees are expected to behave in a manner consistent with the Company Values and comply with the Company's policies, procedures, plans, guidelines, and standards at all times.

The IT team will verify compliance with this Policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner. Employees

must not engage in conduct or activities that are prohibited under this Policy. A breach of this Policy is a serious matter and, therefore, may lead to disciplinary action ranging from counselling or a warning, up to termination of employment, depending on the severity of the breach. If an individual breaks the law, they may also be held personally liable for their actions.

5. IT ACCESS PRIVILEGES

- Employees may be given access to IT resources in order to fulfil their job roles. Access must be requested by an authorised person by logging a request with the IT Department and completing the designated form. The Department Manager's approval is required in all cases. The Syrah IT Department is contactable via email at ITSupport@syrahresources.com.au

- Access to IT resources is strictly for use by the designated Employee only. Sharing IT access credentials with other people is prohibited except with prior permission from the Company's IT Manager.

- If an Employee suspects IT access privileges have been shared contrary to this Policy, they must report it immediately to their Manager or an IT representative.

- Mandatory CyberSecurity, IT training and Simulations forms parts of IT access privileges.

- IT access privileges will be subject to periodic review by the IT Department to ensure they remain appropriate for the Employee's current role. Access privileges will be revoked or adjusted when an Employee changes roles within the Company or leaves the organization, in order to maintain the security and integrity of the Company's IT resources.

6. COMPUTER AND MOBILE DEVICE USAGE

- All IT assets and the data within, remain the property of the Company. IT assets must be treated with respect and maintained in the condition in which they were received. Any incidents involving IT assets, including damage or theft, must be reported immediately to the Employee's Immediate Manager and IT Department with an explanation as to what occurred. If Company IT assets are stolen, this should be reported to the police, and an incident report should be provided to the Immediate Manager and IT Department.

- Employees must abide by the applicable laws regarding their use of IT assets. Any substantiated unlawful use of an IT asset will be met with disciplinary action, which may include termination of employment. Employees must also comply with all Company policies while using IT assets, including, but not limited to, the Code of Conduct, Workplace Behaviour Policy, Social Media Policy and Teleworking Policy. These policies can be found on the Syrah website or for internal policies, on Syrah's SharePoint site.

- Users will not be given local administrator rights on computers.

- Business-related data should not be stored locally on desktop computers, laptops or mobile devices. Instead, it should all be stored on network resources such as authorised shared drives, cloud services or other resources (such as Pronto). This is because network resources are backed up, but local desktop folders are not.

- Users must lock their computers when away from the device. This is to reduce the likelihood of unauthorised access to sensitive data or assets.

- Company mobile devices connected to Company resources will be wiped by the IT Department when the Employee leaves the business.

- Removable media such as USB drivers may not be connected to or used in Company-owned computers without the explicit permission of the IT Department. This is to reduce the likelihood of cyber security breaches through compromised devices.

- Zscaler and other antivirus and security software must not be disabled by Employees. This is to reduce the likelihood of cyber security incidents through malware.

- Company laptops, Company mobile devices, and other Company IT assets must not be used by anyone other than the users for whom they are intended (e.g. family members).

- All Company IT assets must be correctly disposed of by the IT Department when no longer required (i.e. do not just throw them in the bin). The IT Department will securely erase or destroy them so data cannot be recovered.

7. INTERNET USAGE

- Employees must ensure that the Internet is used in a responsible, ethical, and lawful manner and that usage complies with all relevant Company policies.

- Some websites, services and applications may be automatically blocked on Company devices. If an Employee believes that they require access to a blocked service to fulfil the requirements of their role, they must log a request with the IT Department, with Immediate Manager approval attached.

- The IT Team will log and monitor Internet use from all computers and devices connected to the corporate network.

- Daily reports are generated and scrutinised by the IT Department to identify excessive or forbidden Internet usage.

- Peer-to-peer software (such as torrent downloaders) is not permitted on Company resources. This is to avoid wasting business resources on non-business tasks and also to reduce the risk of malware entering through unapproved software.

- All webmail, streaming and social media services are blocked when using Company networks unless approved for official Company related matters, e.g. marketing, branding, etc. These services are allowed when using external Internet.

- Internet access may be revoked due to non-work-related activity when using Company networks at department managers' discretion.

- Employees must not intentionally or recklessly access or transmit computer viruses and similar software through suspicious websites will lead to disciplinary action.

- Employees using the Internet are not permitted to copy illegally and/or wrongfully, transfer, rename, add, modify or delete protected works, information or programs.

- Visitors may be granted access to Syrah's Internet connection on a case-by-case basis as requested by the Department Manager and approved by IT Management. The rules and guidelines in this Policy apply to visitors when using Syrah's IT infrastructure.

- Users of the Internet who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The Company cannot be held responsible for any loss of personal information or any consequential loss of personal property.

8. APPROVED SOFTWARE

- Employees may not install software on Company's computing devices operated within the Company network. Only the IT team can install software on the computer of a user.

- Software must be selected from an approved software list maintained by the IT Department. If a user requires unapproved software to be installed on Company IT assets, the user must immediately report it to the IT Department, which will evaluate if it can be installed or not.

- Any software development or modification must be approved by the IT department, which is responsible for all software deployment.

9. EMAIL USAGE

- Electronic mail (email) is commonly used for business purposes and is often the primary communication and awareness method within an organization. Misuse of email can pose many legal, privacy and security risks; thus, it's important for users to understand the appropriate use of electronic communications.

- All use of email must be consistent with the Company Values, policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

- All mailboxes must have multi-factor authentication (also called "2FA") enabled as a minimum security measure. The 2FA must be configured by the IT Department immediately upon mailbox creation, using the mobile application ("app") as the main authentication method.

- Credit card details and passwords must never be communicated by email. This is because emails are stored indefinitely, and the credit card details/passwords will be vulnerable in the event of a future cybersecurity breach. Use SMS or a phone call (preferred) instead.

- Company email accounts should be used predominantly for Company business-related purposes; personal communication is permitted on a limited basis, but non-Company-related commercial uses are prohibited.

- Files larger than 5 megabytes (MB) are not to be sent by email. Use OneDrive to share the file.

- Suspicious emails, spam or phishing attempts must be reported as spam directly in Outlook. Any concerns can be reported to the IT Department for investigation.

- Do not open links in emails unless sent from a known, trusted user in relation to an expected communication.

- Sender domains should be verified and the IT Department should be contacted if unsure.

10. INTERNAL SECURITY

- User accounts are set to automatically lock after 5 incorrect login attempts.
- If a user suspects that an IT asset has been breached, the user must change the password and report it to the IT Department immediately.
- Minimum password length, history and complexity requirements will be enforced in Active Directory. The password must be changed every 12 months as a minimum, must contain at least 8 digits, at least one upper case letter and one lower case letter, must have at least one special character, at least one number and should not be the same or similar to passwords used previously.
- Physical access to all Syrah server rooms is restricted to IT staff only unless approved by the IT Department.

11. EXTERNAL SECURITY

- All Company network sites will be protected by a firewall with appropriate integrated security measures.
- All computers must be protected by the proxy VPN (Zscaler) and Antivirus (SEP) provided by the Company.
- If a user suspects that a phishing link or other malware has been opened, the user must IMMEDIATELY turn the computer off at the power point and report it to their Immediate Manager and the IT Department.

12. FILE SYNCHRONISATION SOFTWARE

- File synchronisation software is not to be used for Company data without prior approval from the IT Department. This includes iCloud, Box, Google Drive, Dropbox and personal OneDrive subscriptions.
- Syrah's Microsoft OneDrive for Business is permitted for storing work-related data.

13. REMOTE ACCESS

- Only staff that have obtained approval from the relevant Department Manager will be given access to Syrah network resources from outside of the Company network (e.g. by SSL-VPN connection).
- Contractors or other external parties will not be given remote access to Company networks unless approved by IT Management.

14. USING PERSONAL DEVICES (BYOD – BRING YOUR OWN DEVICE)

Personal devices are not to be connected to the Company network without prior authorisation from the IT Department. This includes laptops, phones, tablets, etc.

15. POLICY REVIEW

This document will be reviewed periodically and updated in line with business and legislative requirements.

Syrah Resources Limited			
Title	Information Technology Policy		
Level of Confidentiality	Group Policy	**Revision**	4
Document Status	In Use	**Language**	English
Last Review	September 2024	**Next Review**	September 2025

This Revision	
Author(s)	Stefan Rheeder – Information Technology Manager Agnaldo Laice – GM Institutional Relations & Corporate Services
Authorised Reviewer(s)	Policy Owner and Executive Committee (ExCo)
Authorised Approver(s)	Audit & Risk Committee (ARC) and Board of Directors (BoD)
Legal Review	Andrew Komesaroff – General Counsel
Document Control	Jemma Pititto – Executive Assistant

Revision History

Author(s)	Reviewer(s)	Approver(s)	Revision Number	Status	Revision Date	Description
A. Flemming	D. Corr	D. Strange	0	Superseded	Dec 2016	New Document
A. Ussene T. Dall	S. Rheeder	S. Wells	1	Superseded	Nov 2020	Revision
S. Rheeder A. Laice	SLT & ExCo	ARC & BoD	2	Superseded	Aug 2022	Revision
S. Rheeder A. Laice	SLT & ExCo	ARC & BoD	3	Superseded	Sep 2023	Revision
S. Rheeder A. Laice	Policy Owner & ExCo	ARC & BoD	4	IFU	Sep 2024	Revision