Information Technology Policy

SYRAH RESOURCES

www.syrahresources.com.au

enquiries@syrahresources.com.au

03 9670 7264

CONTENTS

1. INTRODUCTION

Syrah Resources ("Syrah" or "the Company") is an Australian Stock Exchange listed industrial minerals and technology company with its flagship Balama Graphite Operation in Mozambique and a downstream Battery Anode Material Project in the United States. Syrah's vision is to be the world's leading supplier of superior quality graphite 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 and to confirm the responsibilities of employees in relation to IT usage.

This Policy provides clarification in relation to the use of work devices, the use of personal devices on Company networks and the escalation process for IT-related issues.

3. SCOPE

This Information Technology End User Policy (Policy) applies to all Syrah Group employees, embedded consultants 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.

For the purpose of this Policy, "IT resource" or "IT asset" refers to any computer, network resource, Wi-Fi, mobile device, or other IT equipment provided by the Company for Employees to carry out their job functions. 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.

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 all substantiated breaches will 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

1. Employees may be given access to IT resources in order to fulfil their job role. 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

2. Access to IT resources are for use by the intended Employee only. Sharing IT access credentials with other people is prohibited except with prior permission from a Company IT representative.

3. 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.

6. COMPUTER AND MOBILE DEVICE USAGE

1. All IT assets 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 provided to the Immediate Manager and IT Department.

2. Employees must abide by the applicable laws regarding their use of IT assets. Any 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 the Code of Conduct, Workplace Behaviour Policy, Social Media Policy and Teleworking Policy.

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

4. 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 desktop computers and laptops are not.

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

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

7. USB drives must NOT be connected to Company computers unless they are approved by the IT Department. This is to reduce the likelihood of cyber security breaches through compromised devices.

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

9. 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).

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

7. INTERNET USAGE

1. Employees are responsible for ensuring that the Internet is used in an efficient, ethical, and lawful manner, and that usage complies with all relevant Company policies.

2. 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.

3. Internet access will be logged and monitored, even if the device is not being used at a Company site.

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

5. 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.

6. All webmail and streaming services are blocked when using Company networks. These services are allowed when using external Internet.

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

8. Intentionally or recklessly accessing or transmitting computer viruses and similar software through suspicious websites will lead to disciplinary action.

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

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

8. APPROVED SOFTWARE

1. Users are not administrators on their computers, only IT is to install software in the computer of a user.

2. If a user believes unapproved software may have been installed on Company IT assets, the user must immediately report it to the IT Department.

3. Any software development or modification must be approved by IT department. IT is responsible for any new or existing software deployment.

9. EMAIL USAGE

1. 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.

2. 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 cyber security breach. Use SMS or a phone call instead.

3. Company email accounts must be used predominantly for work-related purposes.

4. Files larger than 10 megabytes (MB) are not to be sent by email. Use OneDrive to share the file.

5. 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.

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

10. INTERNAL SECURITY

1. User accounts are set to automatically lock after 5 incorrect login attempts.

2. 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.

3. 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.

4. Physical access to all Syrah server rooms are restricted to IT staff only, unless approved by IT Department.

11. EXTERNAL SECURITY

1. All Company network sites will be protected by a firewall with appropriate integrated security measures.

2. All computers must be protected by the proxy VPN (Zscaler) provided by the Company.

3. 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 the user’s Immediate Manager and the IT Department.

12. FILE SYNCHRONISATION SOFTWARE

1. 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.

2. Syrah’s Microsoft OneDrive for Business is permitted for storing work-related data.

13. REMOTE ACCESS

1. Only staff that have obtained the 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).

2. 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 allowed 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		
Document No.	[Abstract]	**Revision**	1
Document Status	IFU	**Language**	English
Last Review	November 2020	**Next Review**	November 2021
Level of Confidentiality	Group Document		

This Revision	
Author(s)	Adonis Ussene – Information Technology Superintendent Tristan Dall – Information Technology Consultant
Authorised Reviewer(s)	Stefan Reeder – Information Technology Manager Andrew Komesaroff – Senior Legal Counsel
Authorised Approver(s)	Stephen Wells – Chief Financial Officer

Revision History

Author(s)	Reviewer(s)	Approver(s)	Revision Number	Status	Revision Date	Description
A. Flemming	D. Corr	D. Strange	0	IFU	5 Dec 2016	New Document
A. Ussene T. Dall	S. Rheeder	S. Wells	1	IFU	19 Nov 2020	Revision