Cyber Security Policy

Purpose

This policy provides the basis of cybersecurity management within Federation Mining (The “Company”) and applies to all personnel and information systems and information assets used by, or on behalf of Federation Mining, including those managed or hosted by third parties

Effective protection of business information & systems is critical, both in the ability to preserve the reputation of Federation Mining and in reducing the risk of the occurrence of negative events and incidents.

Federation Mining is a member of the Australian Cyber Security Centre (ACSC) which provides regular security threat assessments and updates. This policy was prepared based on guidance material from the business cyber security guide.

Definitions

“Personnel” shall mean:

- all directors, senior executives, employees and officers of the Company;
- contractors (including sub-contractors) occupying permanent or part time fixed term contracts;
- consultants or suppliers of goods or services and their staff; or
- third parties including intermediaries and associates.

Administrator shall mean the individual responsible for coordination of IT information systems which is the Executive Assistant based in Sydney office.

ACSC shall mean the Australian Cyber Security Centre which is a department of the Australian Government Defence Signals Directorate.

Scope
This policy applies to all Federation Personnel.

Policy framework

Cyber Security Principles

Personnel are required to follow these best practice steps:

- Keep all electronic devices' passwords secure and protected
- Logging into accounts should only be performed through safe networks and approved applications and software
- Install security updates and upgrade antivirus software as required by the company administrator
- Never leave devices unprotected and exposed and lock computers when leaving the desk
- When working remotely, all the cybersecurity policies and procedures must be followed and still apply
- Personnel must not attempt to turn off or circumvent any security measures.
- Personnel must report any security breaches, suspicious activities or issues that may cause a cyber security breach to the administrator
- Federation Mining may report cyber security incidents to the ACSC reporting line for investigation if required

Device Security and Using Personal Devices

- All devices owned and/or provided by Federation Mining must have an approved antivirus and fire wall software installed. This subscription is managed by the company administrator.
- Logging in to any work accounts for personal devices such as mobile phones, tablets or laptops, can put Federation Mining data at risk. Use of personal devices must be approved and completed in accordance with the mobile phone & device procedure.

Password Requirements

To avoid employee work account passwords being compromised, these best practices are required for setting up passwords:

- Use at least 8 characters (must contain capital and lower-case letters, numbers and symbols)
- Do not write down password and leave it unprotected
- Do not exchange credentials when not requested or approved by supervisor
- Change passwords every 90 days or earlier if directed by the administrator

Email Security

Emails can contain malicious content and malware. In order to reduce risk, Personnel should employ the following strategies:

- Do not open attachments or click any links where content is not well explained
- Check the email addresses and names of senders
- Search for inconsistencies
- Block junk, spam and scam emails
- Avoid emails that contain common scam subject lines such as prizes, products and money transfers
- If an employee is not sure that an email, or any type of data is safe, the employee should contact the administrator

Transferring Data

Data transfer is a common cause of cybercrime. Personnel should follow these best practices when transferring data:

- Avoid transferring personal information such as customer data and employee information
- Adhere to the relevant personal information legislation
- Data should only be shared over authorised networks
- If applicable, destroy any sensitive data when it is no longer needed

Acceptable Use

- User accounts on work systems are only to be used for the business purposes of Federation Mining and not to be used for personal activities

- Personnel are responsible for protecting all confidential information used and/or stored on their accounts. This includes their user logins and passwords. Personnel are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised persons outside of Federation Mining
- Personnel must not purposely engage in any activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to Federation Mining systems for which they do not have authorisation

Oversight and enforcement

The implementation of this policy will be monitored by the Vice President responsible for Human Resources and the Board will be provided regular reports on progress and performance. The security and update status of Federation Mining systems will be regularly checked and tested by a third party IT consultant.

This policy must be read in conjunction with the following documents:

- Federation Mining Code of Conduct
- Data Privacy Policy
- Mobile Phone and Device Procedure
- Federation Mining approved software and application register

This policy position will be reviewed annually as a minimum and when required by legislative changes.

Signed: S.M. Le Messurier

Mark Le Messurier

Managing Director

November 2021