Cyber Security Policy

While Gateway Mining Limited (**Gateway** or the **Company**) wishes to foster a culture of openness, trust, and integrity, this can only be achieved if external threats to the integrity of the Company's systems are controlled and the Company is protected against the damaging actions of others.

1. Purpose

1.1 This policy sets out guidelines for generating, implementing and maintaining practices that protect the Company's cyber media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

1.2 This policy applies to directors, officers, employees, contractors and consultants of the Company, including all personnel affiliated with third parties, to all equipment owned or leased by the Company, and to all equipment authorised by Gateway for the conduct of Gateway's business.

2. Policy

2.1 While Gateway wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the Company's systems remains the property of the Company. Because of the need to protect Company's network, the confidentiality of information stored on any network device belonging to the Company cannot be guaranteed, and the Company reserves the right to audit networks and systems periodically to ensure compliance with this policy.

2.2 Information in the possession of the Company shall be classified into different grades depending on its degree of confidentiality. Particularly sensitive information will receive special protection.

2.3 Employees and volunteers will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

2.4 Breach of this policy by any employee or individual to which this policy applies may result in disciplinary action, up to and including dismissal.

3. Responsibilities

3.1 It is the responsibility of the Managing Director and the Company Secretary to ensure that:

- staff are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately; and
- a cyber security officer is appointed.

3.2 It is the responsibility of the cyber security officer to ensure that:

- the Managing Director and Company Secretary are kept aware of any changes to the Company's cyber security requirements; and
- a summary on the Company's cyber security status is submitted annually to the board.

3.3 It is the responsibility of all individuals to which this policy applies to ensure that:

- they familiarise themselves with cyber security policy and procedures;
- their usage of cyber media conforms to this policy.

3.4 In the event of any uncertainty or ambiguity as to the requirements of the cyber security policies or procedures in any particular instance, individuals should consult the Company Secretary of Managing Director.

4. Processes

Monitoring

4.1 The Managing Director may authorise individuals with responsibility for cyber security issues in the Company, including the cyber security officer, to monitor the Company's equipment, systems and network traffic at any time for security and network maintenance purposes.

Confidentiality

4.2 Following consultation with the cyber security officer, the Managing Director shall from time to time issue cyber security procedures appropriate to different levels of confidentiality.

4.3 The Company shall classify the information it controls in the Company's computer system files and databases as either non-confidential or confidential (in one or many categories).

4.4 The cyber security officer is required to review and approve the classification of the information and determine the appropriate level of security that will best protect it.

System taxonomy

Security level	Description	Example
Red	This system contains confidential information – information that cannot be revealed to personnel outside the company. Even within the company, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have an adverse financial impact on the business of the company.	Cloud-server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information. Can include stand-alone laptops that have synchronised copies of cloud-server data
Green	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access server and application(s). Management workstations used by systems and network administrators.
Black	This system is externally accessible. It is isolated from RED and GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public web server with non-sensitive information.

Data taxonomy

Security level	Description	Example
Red	shareholder data allowing financial exploitation or identity theft Company data allowing banking or financial exploitation	Company credit card and banking data Material exploration data not in the public domain
Green	Personnel data allowing address or email exploitation Company intellectual property that has financial or reputational consequences	Addresses that would facilitate spamming Internal emails
Black	Publicly accessible data	Non-sensitive information

Access control

4.5 Individuals shall be assigned clearance to particular levels of access to the Company's information resources, and shall access only those recourses that they have clearance for. Access control shall be exercised through username and password controls.

Computer security

4.6 All PCs, laptops and workstations should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

4.7 Users must keep passwords secure. Accounts must not be shared, and no other people may be permitted to use the account. Passwords should not be readily accessible in the area of the computer concerned. Authorised users are responsible for the security of their passwords and accounts.

4.8 Users who forget their password must contact the relevant IT department or supervisor to get a new password assigned to their account. The user must identify themselves appropriately.

4.9 Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorised users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

4.10 Users will not be allowed to log-on as system administrators. Users who need this level of access must contact their immediate supervisor or the managing director.

4.11 Employee log-on IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, or otherwise leaves the employment of the Company. Supervisors/managers shall immediately and directly contact the IT support provider to report change in employee status that require terminating or modifying employee log-on access privileges.

4.12 Special permissions are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the Company and require the permission of the Company's cyber security officer and/or the Managing Director. Monitoring of the special permissions shall be undertaken via a register kept by the cyber security officer showing who currently has special permissions, for what reason, and when these permissions will expire.

4.13 All computers and devices used by the user that are connected to the Company's internet/intranet/extranet, whether owned by the user or the Company, shall be continually executing virus-scanning software with a current virus database approved by the cyber security officer or the Managing Director.

4.14 Malware protection software must not be disabled or bypassed, nor the settings adjusted to reduce their effectiveness.

4.15 A record of the antivirus and anti-malware software will be kept by the Company.

4.16 Company data stored on laptops that may leave the Company's premises must be protected by encryption or passwords.

4.17 Alternatively, staff who need access to sensitive data offsite should be given remote access privileges subject to adequate safeguards.

4.18 Computers being deaccessioned (whether for sale, reuse or disposal) shall not be released until all data has been securely deleted.

4.19 Users shall not download unauthorised software from the internet onto their PCs or workstations.

4.20 Users must use extreme caution when opening email attachments received from unknown senders; these may contain viruses and/or malware.

4.21 Users who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the cyber security officer, the Managing Director or the Company Secretary immediately.

4.22 Users must not themselves breach security or disrupt network communication on the Company's systems or elsewhere. Security breaches include accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties. "Disruption" includes network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.23 Users shall not attach unauthorised devices to their computers unless they have received specific authorisation from their manager or the company IT designee.

4.24 Users shall not attach to the network non-company computers that are not authorised, owned or controlled by the Company.

4.25 Users must follow data retention and disposal procedures to ensure compliance with legal and regulatory requirements.

Cloud Access and Security

4.26 Only authorised employees and users are permitted to access company information stored on the cloud. Access will be granted based on the principle of least privilege.

4.27 Multi-factor authentication (MFA) must be used to access cloud-based systems and data.

4.28 Regular backups of critical data stored on the cloud must be performed and securely stored in accordance with the company's backup Policy.

4.29 Employees must ensure that all devices used to access cloud-based systems are regularly updated with the latest security patches and antivirus software.

Compliance

4.30 Employees must comply with all relevant legal and regulatory requirements, including the Privacy Act 1988 (Cth), Corporations Act 2001 (Cth), and Taxation Administration Act 1953 (Cth), when accessing and handling cloud-stored data.

5. Insurance

The Company confirms that is currently has Cyber Liability and Privacy Protection Insurance in place to cover the Company in scenarios where a cyber security breach is to occur. The Company will maintain insurance cover in relation to cyber security risks and the board will evaluate annually whether or not the level of cover requires modification.

6. Policy Review

The Company's cyber security risk management system is evolving. It is an on-going process and it is recognised that the level and extent of the risk management system will evolve commensurate with the development and growth of the Company's activities. The Board will review this policy annually and determine if any changes or amendments are required to the policy.