IT AND ACCEPTABLE USE POLICY

1. PURPOSE

The purpose of this Policy is to define the appropriate use of Company information and Systems by Users within Lincoln Minerals Limited (Company).

ACCEPTABLE USE POLICY

This policy includes the information protection requirements common to all Users of Company information and systems.

POLICY STATEMENT

All Systems and any Company information or messages stored on them or created, sent, or received using them, are the property of the Company. It is each User's responsibility and obligation to ensure that Systems are used properly. All Users must be trained on the Acceptable Use Policy at least every three years. A violation of this Acceptable Use Policy may result in disciplinary action up to and including termination of employment or termination of service contract. Violation of this policy may also be a violation of other Company policies or procedures, including, but not limited to the Company Code of Conduct.

Business Use of Company Systems

Personal use

Systems are to be used to conduct Company business. Occasional personal use of Systems is permitted, however, as long as it does not: (1) impact the performance of activities related to the discharge of the User's responsibilities to the Company; (2) violate this Acceptable Use Policy or any other Company policies or procedures; and (3) violate any applicable laws.

Such occasional personal use is subject to all terms of this Acceptable Use Policy, including monitoring.

Users shall only install applications or software on Company Systems that are authorized by Information Technology adviser.

Acceptable use of electronic communication

Users shall use Company electronic communication systems and services in accordance with Company policies and procedures. Electronic communication systems and services include but are not limited to: Internet; electronic mail and services such as text messaging; electronic publishing services such as blogs, podcasts, and wikis; web forums such as bulletin boards, discussion groups, and news groups; Internet collaboration services such as electronic mail, chat, instant messaging, telephony, web conferencing, and file sharing.

Sharing of non-public Company information is allowable subject to the following conditions:

Users shall not use or disclose to others, without prior written consent of the Company, any non-public information related to the Company or the Company's business.

Authorised uses of personal information shall be limited in accordance with normal privacy protocols.

Third Parties that will be exposed to Company classified information shall sign a non-disclosure agreement. Users shall not disclose, share or transmit Company classified information with Third Parties unless approved by the business owner.

Users shall only use Internet collaboration services (such as, but not limited to, electronic mail, instant messaging, chat, telephony, video conferencing, file sharing, etc.) on Company Systems that are authorized by Information Technology.

Acceptable use of Internet

Internet access originating from the Company network must go through a Secure Access Zone (SAZ) or other related protection technology architecture approved by the information protection

organization. Use of commercial Internet services (e.g., mobile hotspots, mobile broadband cards, air cards, USB modems, etc.) to access the Internet while connected to the Company network is prohibited.

Users shall transmit Company classified information in accordance with standard protection measures.

Users shall not load, download or install software from the Internet on Company Systems without the approval of Information Technology. Information Technology shall authorize software for use by Users.

Subject to applicable law, Users shall not use Company Systems to access Internet websites where the content, process or service interferes in the secure operation of Company Systems.

Acceptable use of electronic mail

Users must prepare Company e-mails with the same degree of accuracy, care, and propriety that they would use in the creation of traditional written communications. Users shall be aware that statements made through electronic communications may be legally binding.

Users shall not use Company e-mail to perform the following activities:

- Send or forward chain letters;
- Send or forward security related messages not originating from the information protection organization (e.g., computer virus warnings) unless done in support of an investigation.

Company e-mail shall not be automatically forwarded to non-Company systems unless approved by the information protection organization. Non-Company systems include, but are not limited to: home or personal computers; public Internet terminals; file transfer servers; web-based storage, backup, and file sharing resources; collaboration platforms, etc. Company information shall be protected in accordance with the standard protection measures.

E-mail messages containing Company information classified Highly Restricted shall be encrypted during transit across public communications networks.

If a Company e-mail message containing classified information is received in error, the receiver must notify the sender of the error and delete the message.

Users must immediately contact Company legal counsel upon receipt of a message that contains illegal or anti-competitive business-related information or information that violates Company policies or procedures. Legal counsel will assist Users in preparing an appropriate response so as to safeguard the Company from being accused of illegal or anti-competitive conduct.

Users shall exercise caution when discussing Company classified information in a public setting.

The host of a conference call shall ensure that only authorized individuals are connected to the call via the use of distributed pass codes for entry to the conference call.

Further use restrictions

Users may not use any System:

- In a manner that would violate confidentiality or any other Company policy or procedure or any law or regulation;
- In a manner that would reflect badly upon the Company, such as by pirating software, stealing copyright material, stealing passwords, hacking, participating in the viewing or exchange of pornography or other obscene materials, or engaging in any other unethical or wrongful conduct;
- To load, download, or store games or non-Company related or other unauthorized executable files;
- To participate in non-Company related business activities;
- To participate in gambling;
- For the purpose of solicitation, such as requesting contributions or soliciting memberships to non-Company approved charitable organizations or soliciting political candidates;
- For attempted financial gain resulting from knowledge of Company classified information;
- In a manner that would cause a reasonable person to be defamed, offended, harassed, or disrupted, such as by uploading, downloading, or transmitting sexual comments or images, racial or ethnic slurs, or other comments or images that would offend someone on the

Level 14, 333 Collins Street
Melbourne Victoria 3000

info@lincolnminerals.com.au
www.lincolnminerals.com.au

basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability;
- To enable unauthorized Third Parties to have access to or use any Systems or otherwise jeopardize the security of any Systems;
- To publicly comment or speculate on Company performance, policies or actions;
- To post Company classified information on any public Internet sites (such as chat rooms, discussion forums, and newsgroups) unless it is part of their assigned job function; or
- In a manner that would significantly impact the performance, capacity, or integrity of any System.

A user's possession, development, or intentional use of malicious software, hacker tools or other security-related software is prohibited.

Only software authorized by Information Technology shall be installed on any System. Users shall not install software onto any System without the approval of Information Technology. Information Technology shall authorize software.

Users must not attempt to circumvent or otherwise alter the security of any System.

Company's Right to Monitor Systems

Subject to applicable law, the Company may monitor any System and any User's use of any System.

Internet usage, will take place only where required in the Company's legitimate interest.

These interests include:

- Ensuring effective and/or secure operation of any System;
- Keeping records of transactions in which the Company is involved;
- Ascertaining Employee compliance with applicable laws and Company policies or procedures; or
- Detecting, preventing or investigating crime.

Monitoring will be in accordance with applicable Company procedures and applicable legal requirements. Any data gathered as a result of monitoring activities will be processed in accordance with applicable law and may be disclosed outside the Company in support or as part of investigations or legal proceedings.

Except as protected by applicable law, communications on Systems are not private. Passwords and user IDs are designed to protect the Company's business information from unauthorized access, not to provide Users with personal privacy in any communications.

User Responsibilities

Password use

Users shall change their password from the initial System default upon the first use of their user ID.

Users shall create strong passwords that are a minimum of 8 characters in length and be comprised of letters, numbers, and special characters.

Passwords shall not be easily associated with the Company or the User (e.g., Social Security Number, employee number, address, numerical equivalent of name, family names, pet names). Passwords shall not contain words from a dictionary, movie, geographical location, mythology, Company products, customers, or application names. Also, passwords shall not be based upon month/year combinations.

Users shall change passwords at least every 90 days.

Passwords shall not be saved using the AutoComplete feature, or other automated password storage mechanism, in Web browsers and applications.

Users shall create strong passcodes, or personal identification numbers (PIN), for devices or equipment used to access Company Systems and information. Default passcodes shall be changed immediately. Passcodes shall not be comprised of the telephone extension, date of birth, anniversaries, portions of Social Security or Government Identification Numbers, or sequential numbers.

Level 14, 333 Collins Street
Melbourne Victoria 3000
info@lincolnminerals.com.au
www.lincolnminerals.com.au

Users shall create passwords for access to Company Systems that are different from passwords used for non-Company Systems (such as personal web banking applications, customer or supplier applications).

Unattended user equipment

Users shall use Company Systems and computing devices in a physically secure location and protect them against unauthorized use.

Users shall ensure that their computing devices are physically secured using cable locks or other techniques when unattended.

Clear desk and clear screen policy

Authentication credentials, such as tokens or passwords, must not be stored in the open.

Company classified information, when printed, shall be cleared from printers, copiers, and fax machines.

A user's session on a computing device shall be configured with a password-protected screen-saver. The screen-saver must require the entry of a password or passcode after a device has been left idle for a maximum of 15 minutes. Devices that do not require user interactive sessions (e.g., display only terminals, kiosks) may have the password-protected screen-saver disabled by Information Technology, and shall be subject to approval by the information protection organization.

Users shall manually engage a password-protected screen-saver when their computing device will be unattended.

User access management

All access to Systems containing Company classified information shall be controlled by an authentication method involving a minimum of a unique user ID/password combination.

All activity performed under a user ID is the responsibility of the individual to whom the ID is assigned. Users shall not share their user ID/password with others or allow other Employees to use their user ID/password. Users are not permitted to perform any actions under any user ID other than their own, or a group or shared user ID to which they have been granted access. The use of generic IDs (such as temp or guest), unless specifically assigned to an individual and documented, is not permitted. Group or shared IDs must have a designated owner, in writing, accountable for all actions performed under the group or shared ID.

User's access rights shall be reviewed every six (6) months in order to maintain effective access control. User IDs that have not been accessed for 13 months shall be disabled. User access rights shall be revoked immediately when a User is no longer entitled to them due to, but not limited to, separation, change of employment or transfer within the Company, change or termination of contract or legal agreement.

Privileged access rights to Systems, including administrative access to laptops, workstations, and other computing devices, is restricted to authorized personnel with a business need.

All Users that have access to privileged access rights (such Administrator or Root) shall have their own personal user IDs for normal business use. Privileged Users must use their personal user IDs for conducting non-privileged activities. Wherever possible, privileged Users must login to a System using their personal user ID prior to invoking a privileged user ID.

Information classification and protection

Non-public Company information shall be classified in accordance with Company information classification categories. Information in any format (e.g., hard copy or electronic) shall be protected by all Employees and Third Parties in accordance with standard protection measures at the level commensurate with its value, legal requirements, sensitivity and criticality as determined by the assigned classification.

Users shall encrypt files and removable media containing Company information classified as Highly Restricted and in accordance with the Technical Security Baselines. Removable media includes, but is not limited to, laptops, hard drives, thumb drives, memory cards, USB flash drives, portable media players, or any other electronic information storage device.

Level 14, 333 Collins Street
Melbourne Victoria 3000
info@lincolnminerals.com.au
www.lincolnminerals.com.au

Users shall not store or exchange Company classified information on Third Party or non-Company systems unless a contractual agreement to protect the information exists. Non- Company systems include, but are not limited to: home or personal computers; public Internet terminals; file transfer servers; web-based storage, backup, and file sharing resources; collaboration platforms, etc.

Users, before disposal, shall shred paper records containing Company classified information. The shred size shall be small enough that there is reasonable assurance the information cannot be reconstructed. Other forms of disposal must be approved by the information business owner. Paper records shall be disposed in accordance with the Company's records retention guidelines.

Users shall delete the contents of removable media containing Company classified information and licensed software before reuse or transfer out of their direct control (e.g., transfer to another department, workstation refresh). Users shall ensure that the data contained on the media no longer exists and that the data cannot be recovered or reconstructed. The procedure for removing content shall be coordinated with Information Technology.

Data leakage control

External storage media (floppy disks, CDs, CDR-Ws, zip disks, etc.) that have been out of the control of the User shall be scanned for malicious software before use on Company Systems.

If malicious software is suspected on a System, the User shall disconnect the System from the Company network immediately, notify their local Helpdesk, and assist in the removal of the software prior to any re-connection to other Systems. It is the responsibility of the User, with appropriate technical assistance, to ensure that the malicious software has been successfully removed before resuming communications on any Systems.

Users shall scan all files downloaded from the Internet or received via e-mail from outside the Company for malicious software using the Company approved malicious code detection capability, where available, before use on Company Systems. Attachments or website links contained in messages from unknown senders should not be opened.

Reporting security incidents

Users shall report known or suspected information security incidents or violations of the Information Protection Policy to Senior IT management.

If a User suspects a security weakness, threat or System vulnerability, that individual shall notify IT Management immediately. Only individuals in an information security or audit role, or an authorized designee by the information protection organization shall test security weaknesses. The User is forbidden to test the security weakness without the permission, direction and involvement of the information protection organization. The User shall not publicize the discovered vulnerability or weakness.

Mobile Computing and Teleworking

Mobile computing and acceptable use

Users are responsible for the security and care of mobile computing devices, including, but not limited to laptops, mobile phones, and tablet computers, issued to them or approved for use by the Company (i.e., personally owned devices). If the Company-issued device is lost, stolen or destroyed and the individual responsible for that device is found negligent in its protection, the individual may be held financially responsible for cost incurred by the Company to replace the device. Users shall immediately report the loss of Company information assets to their local IT help or service desk.

Users are not permitted to store Company-related information on personally owned systems or any other equipment not provided by the Company unless approved by the information protection organization and securely configured by Information Technology to protect Company classified information.

Only network devices authorized by Information Technology or authorized designate shall be permitted on the Company network. Network devices covered by this requirement include, but are not limited to, firewalls, routers, hubs, switches, bridges, wireless access points, and other related wired and wireless networking technologies.

Teleworking

Level 14, 333 Collins Street
Melbourne Victoria 3000

info@lincolnminerals.com.au
www.lincolnminerals.com.au

The Information Protection Policy applies to all Systems and information regardless of location.

Users shall only use Company-approved and securely configured Systems to access any Company System. Use of home PCs, personal laptops or other non-Company systems are prohibited unless approved by the information protection organization and securely configured by Information Technology to protect Company classified information. Non-Company systems include, but are not limited to home or personal computers; public Internet terminals; file transfer servers; web-based storage, backup, and file sharing resources; collaboration platforms, etc.

Authorised Company Systems, classified information, and media taken outside Company premises, shall be controlled, secured, and protected to ensure protection against theft, destruction, or unauthorised disclosure and use according to the standard protection measures.

All remote access points into the Company's environment shall be authorized by Information Technology.

FURTHER INFORMATION AND SUPPORT

The Company encourages open communication and dialogue regarding this Policy and any matters which may arise in connection with it.

If you have any questions regarding this Policy or would like further information regarding the processes outlined in this Policy, please contact your relevant manager or:

Name: Andrew Metcalfe
Position: Company Secretary, Lincoln Minerals Limited
Email: andrew.metcalfe@lincolnminerals.com.au

Level 14, 333 Collins Street
Melbourne Victoria 3000
info@lincolnminerals.com.au
www.lincolnminerals.com.au