Chifeng Jilong Gold Mining Co., Ltd.

Information Technology Security System

December 2022

1.0 Purpose

As an operation system guidance document, this system is designed to establish the management direction, and clarify the procedure requirements and technical guidelines, so as to protect the electronic information security of Chifeng Jilong Gold Mining Co., Ltd. (hereinafter referred to as "Chifeng Gold" or "the Company").

2.0 Scope

This system applies to all employees and third-party personnel who use Chifeng Gold's network in Chinese companies, as well as all computer and data communication systems of Chifeng Gold.

The IT Department needs the active participation and support of every user. Every user must receive proper training and have relevant reference materials so that they can correctly protect the assets of Chifeng Gold.

All information security incidents in Chinese companies that are unfavorable to Chifeng Gold must be reported to the Information Technology Administrator immediately.

All electronic information on the network of Chifeng Gold, the internal computer systems and LAN, and computers and networks used by Chifeng Gold to interact with the outside world shall follow this system.

This system mainly includes the following contents:

- Information responsibility
- Information classification
- Security system
- Access control
- Network security
- Workstation and LAN control
- Basic security control
- Information technology service
- Non-compliance reporting

This system defines the bottom line of control. All employees of Chifeng Gold shall be familiar

with this system and follow it.

3.0 Information responsibility

3.1 Legal ownership

3.1.1 Except for materials clearly owned by third parties, the legal ownership of all electronic information stored in and passing through Chifeng Gold's system belongs to Chifeng Gold. Except for the specific written authorization by CEO, all the development business information of Chifeng Gold's employees belongs to Chifeng Gold.

3.2 Information controller

3.2.1 Managers and supervisors are the controllers of electronic business information. A designated controller is required for all electronic information. If an organization does not explicitly designate the information controller, the IT Department shall designate the controller. Information controllers do not have the legal ownership of information, but just management members of Chifeng Gold who can make decisions for the organization. Information controllers or their representatives must decide and perform the following tasks:

- Approve the right to use electronic information.
- Choose special control measures to protect information, such as additional input validation or regular backup process.
- Approve the transplantation of all new systems or upgraded application systems to the application environment.
- Select a level for information, and determine the level and classification of sensitive information.

3.3 Information manager

3.3.1 The information manager must be the personnel from the IT Department who develop, support and conduct electronic maintenance of applications. It is the responsibility of the information manager to ensure that services are provided per this system and information technology standards. The information manager must protect information under the basic security control and information technology security operating system, so that it will not be accessed, used, modified, distributed and destroyed without

permission. The information manager is responsible for performing general control operations such as backup and recovery.

3.4 User

3.4.1 User is defined as anyone who accesses the electronic information of Chifeng Gold. Users shall comply with the security requirements specified by the information controller, information manager or IT Department. They shall also be particularly familiar with all the information technology systems, processes and standards of Chifeng Gold. In case of any questions about how to deal with a particular piece of information, these questions shall be answered by the information manager or controller.

4.0 Information classification

4.1 Chifeng Gold has adopted an information classification system that classifies information into three classes: confidential information, internal information and public information. All information under the control of Chifeng Gold, whether from internal or external sources, can be classified into one of them. Every user shall be familiar with these classifications and must know how to protect information.

4.1.1 Confidential information

Confidential information can only be used within Chifeng Gold with the permission of the information owner. Any disclosure of confidential information without permission may cause harm to Chifeng Gold or its suppliers, business partners or employees. It includes but is not limited to employee performance evaluations, strategic alliance contracts, computer passwords, and internal audit reports.

4.1.2 Internal information

Internal information includes all information that cannot be clearly classified as confidential information. All users can access to this information. Although disclosure of confidential information without permission violates this system, such information will not seriously affect Chifeng Gold. It includes but is not limited to Chifeng Gold’s telephone directory, dial-up access number, new

employee training and internal systems.

4.1.3 Public information

Public information can be disclosed upon approval of the management of Chifeng Gold. By definition, it can be interpreted as that there should be no information published without approval. The release of such information will not cause any harm. It includes but is not limited to product and service brochures, advertisements, recruitment and announcements.

4.1.4 Default class

Any information that is not classified by the information owner will be defaulted to "internal information".

5.0 Security system

5.1 The IT Department will draft new information technology security policies aiming at the Company's objectives and maintain all information technology security policies. The management of Chifeng Gold will review these policies and their changes every year. The Company will also convey the latest information technology security policy to employees every year.

The firstly released *Information Technology Security System* will be sent to all employees through company announcement or email. Chifeng Gold requires all new employees to read the *Information Technology Security System* carefully.

6.0 Access control

6.1 Need to know

6.1.1 Access to information must be granted to the user only when the user "needs to know". Information can only be disclosed to users with reasonable business needs.

6.1.2 To pursue the concept of "need to know", Chifeng Gold adopted the access request approval process. If a new user is to be created, the department manager of that user will send a *New User Access Request Form & Setup Checklist* (Appendix A) to the IT Department, stating the access rights to be granted to the new user. The IT Department will set the access rights of that new user per the request in the form.

6.2 Add the user's right to use

6.2.1 Chifeng Gold has a formal management process for adding user's access rights in the system, including the following steps: access authentication; access authorization; notifying users; providing preset security passwords; and forcing users to change passwords when they log in for the first time.

6.2.2 When a new user requires a domain account and/or email account, the Human Resources Department will send a *New User Access Request Form & Setup Checklist* with the approval of the user's department manager. Upon approval, the completed form will be forwarded to the IT Department to create an account.

6.2.3 If a user needs to access the relevant information in the important application software supporting the financial process (Appendix B), it shall first send the *Request Form for Adding and Changing the Account Permission of Financial System* (Appendix C) per the relevant process. This form will be signed by relevant personnel, and finally archived by the administrator shown in Appendix B.

6.3 Modify the user's right to use

6.3.1 Chifeng Gold has a formal management process for modifying users' access rights in the system, including the following steps: access application; access authorization; and notifying users.

6.3.2 The department manager of the user concerned shall send an email regarding the modification of the user's access rights or submit the *Access & Building Common File Request Form* (Appendix D) to the IT Department. After the IT Department modifies the user's access rights, it will send an email to the user's department manager or return this form to notify the corresponding changes. The IT Department will save the email in the permission document of that user.

6.3.3 The IT Department will not change or modify the user's access rights on the basis of a single phone call.

6.3.4 Administrators in major applications of financial process (Appendix B) shall also follow the above procedures and submit the *Request Form for Adding and Changing Account Permission of Financial System*.

6.4 Terminate the user's right to use

6.4.1 Chifeng Gold has a formal management process for canceling users' access rights in the system, including the following steps: the Human Resources Department notifies the IT Department and administrators in the major applications of financial process (Appendix A); canceling access rights; and regularly comparing the roster of active employees (from HR Department) and information technology system access rights. Administrators in the major applications of financial process (Appendix A) shall check with the relevant department manager whether access rights have been cancelled, or periodically compare the roster of active employees and information technology system access rights.

6.4.2 If an employee leaves, HR Department will send an *Account Suspension/Termination Form* (Appendix E) via email to inform the IT Department and administrators in major applications of financial process (Appendix B). They will review user files to determine what to do about access rights of the separated employee. They will cancel the access rights of the separated employee in all relevant systems, and delete the access rights after one week by default. Finally they will inform HR Department and the appropriate department manager that access rights have been cancelled.

6.5 Review the user's right to use

6.5.1 HR Department sends a roster of active employees to the IT Department on a semi-annual basis. The IT Department will compare the list of active users with this roster of active employees. If it is found that any separated employee still has access rights, this will be confirmed with the department manager of that employee.

6.5.2 Administrators in major applications of financial process (Appendix B) send a list of active users to the relevant department manager on a semi-annual basis to verify whether any separated employee has access rights.

6.6 Privileged account

6.6.1 All users (including IT staff) shall use the local computer by means of access rights.

6.6.2 Users shall not have domain administration rights or enterprise network administration rights under any circumstances.

6.6.3 Even the user accounts of the IT Department shall not have domain administration

rights or enterprise network administration rights. When they need access to a server or program, they shall use a special account with domain administration rights or enterprise network administration rights. These special accounts are controlled by the IT Manager.

6.6.4 Administrator accounts for all applications, operating systems and databases, including administrator accounts in major applications of financial process (Appendix B), shall be created separately and shall not share the same account.

6.7 Contractor's access rights

6.7.1 The department manager in charge of contractor related affairs shall review and approve the contractor's request to access the network of Chifeng Gold and send the corresponding *Access & Building Common File Request Form* to the IT Department. Before granting appropriate access rights to the contractor, the IT Department will check that the contractor's computers are adequately equipped with antivirus software and the latest security patches, and that the date of his signature file is the latest. Any access will be denied unless the above conditions are met.

6.7.2 The department manager in charge of contractor related affairs must ensure that the contractor will not access the network of Chifeng Gold without approval (See "10.0 Non-Compliance reporting"). Once it is verified that such unauthorized access has occurred, IT Department shall be notified, and it will immediately stop such connection to the contractor and report such unauthorized access per the *Information Technology Policy on Non-Compliance*.

7.0 Network security

7.1 Password management

7.1.1 Choose a password

Users shall choose passwords that are not easy to guess. Passwords cannot be found in dictionaries and shall not contain any private information.

7.1.2 Within application and software permissions, the password shall be set as follows:

7.1.2.1 A default password is given when setting up a new user. The default password should be changed to a new password when the user logs in for

the first time. Passwords must have at least 6 characters. The new password cannot be the same as the password used five times before and must be changed every 181 days. The cycle of password change must be set at least 45 days. The account will be locked automatically after five login errors and failures, and users must enter the correct password 30 minutes later to unlock it.

7.1.2.2 For users of major applications of financial process (Appendix A), their passwords shall contain a minimum of 6 characters and shall be a combination of numbers and letters. It is forbidden to use the same password again. Such users shall change their passwords at least every 121 days. If the login fails 5 times, the account will be automatically locked, and only the administrator in major applications of financial process can release the locked state. If the user forgets the password that needs to be changed or reset, his department manager shall send an email to the administrator in major applications of financial process to make the relevant request.

7.1.2.3 If the user suspects that someone else knows his/her password, he/she must change it immediately.

7.2 Users shall not be able to disclose their passwords to anyone, including IT staff. If a user discovers that his/her password has been stolen, he/she must immediately notify the IT Manager.

Users are not allowed to store passwords in computer files or computer programs unless the passwords are encrypted with approved software. Users are not allowed to write down their passwords.

7.3 Users shall always make sure that they log out or lock their computer before leaving their seat to prevent others from accessing their computer.

7.4 The IT Manager periodically reviews inactive accounts. All accounts without any activity within 60 days will be suspended.

7.5 When users return to Chifeng Gold after a long holiday (e.g. more than 60 days), their direct

supervisor must contact the IT Department for approval before the user's right to use can be restored.

7.6 Remote access

7.6.1 Hardware approval

In case of remote access to the computer network of Chifeng Gold, the hardware used must be licensed by the IT Department. All devices must be set up and protected per the guidance of information technology security operation system. It is the responsibility of users to ensure that the hardware configuration is not altered without the permission of the IT Department.

7.6.2 License for remote access

License for remote access to Chifeng Gold's network is only granted to customers with reasonable business needs. The user's immediate supervisor must help the user apply for permission to access Chifeng Gold's network remotely from the IT Department.

All users who make remote access must abide by the regulations on remote access, and shall have participated in remote access training before getting the right to remote access.

7.6.3 Authentication of remote access

SecureID or e-Cert (e.g. CISCO VPN certificate) is required for remote access. Other remote access methods will not be approved.

7.6.4 Handling of confidential information

Electronic confidential information shall not leave the office of Chifeng Gold without security. If confidential information needs to leave the office of Chifeng Gold, it must be protected by encryption software approved by the IT Department. All electronic confidential information transmitted over public networks must be protected with encryption software approved by the IT Department.

7.7 Firewall security

All connections between the internal network of Chifeng Gold and the Internet or other

publicly accessible computer networks must be secured by firewall. If certain programs require ports to be opened on the firewall, these ports must be secure and approved by the IT Manager in China. Under no circumstances should the firewall be opened or reset if the security of ports used by these programs is not guaranteed.

8.0 **Workstation and LAN control**

8.1 Information security for workstations

8.1.1 Control of right to use

Users shall always make sure that they log out or lock their computer access before leaving their seat to prevent others from accessing their computer.

As a supplementary control, the screens of all workstations shall be set to automatically lock the screen if there is no activity for 15 minutes and the password shall be re-entered before login.

8.1.2 Antivirus software

All workstations must be installed with real-time antivirus software.

Users of Chifeng Gold have the responsibility to ensure that the settings of real-time antivirus software have not been modified. When a user discovers a virus, he/she must immediately stop all operations and disconnect the network, and immediately notify the IT Department.

Antivirus software settings in general workstations are unchangeable and only IT staff can change the settings.

8.1.3 Standard application software

Chifeng Gold has a list of licensed software that lists which software can be installed on each employee's computer. Users shall not load software off this list unless it has been tested by the IT Department and it complies with the standard business procedures of Chifeng Gold. Unapproved software will be cancelled without any notice. Acts and conditions that do not conform to the system will be reported.

(See "11.0 System violation reporting").

8.1.4 Hardware changes

Users shall not modify the computer equipment provided by Chifeng Gold without

informing and obtaining the approval of IT Department.

8.2 LAN control

8.2.1 Active network port

Those active network ports that can be connected to public places (not limited to the company lobby, canteen and public meeting room) through Chifeng Gold's network must be immediately prohibited.

8.2.2 Install devices on the network

Only the device set up by Chifeng Gold may connect to Chifeng Gold's network.

9.0 **Basic security control**

9.1 Access to data centers and other sensitive areas is restricted to authorized employees only.

9.1.1 The user access list is reviewed semi-annually by the management department to ensure that users have reasonable causes for business access.

9.1.2 Any extra keys must be locked in the administration office. The keys kept by HR Department may be lent to those who have forgotten keys, contractual employees and emergency personnel (e.g. fire brigade, plant guard) if necessary.

9.1.3 The IT Manager must be notified of the release or use of extra keys.

9.1.4 Access records must be kept in the room where the server is located. In addition to IT staff, the name, date and time of the visitor shall be recorded in the access records.

9.1.5 The management department reviews access records on a monthly basis for abnormal access. In case of no access record due to system restrictions (e.g. enter with a key instead of swiping a card), visitor records will be the primary evidence.

10.0 **Information technology services**

10.1 Email

10.1.1 Email sharing and forwarding

Electronic accounts and user identities assigned to individuals are for personal use only and cannot be shared with others. If a user needs to go on vacation or does not need to check their email for a long time, his/her email will be forwarded to another internal user. It is not allowed to forward confidential information outside Chifeng

Gold. If confidential information is included in an email, the user cannot forward the email to others, unless the recipient has the right to read the information or gets permission from the originator who sent the email.

10.1.2 Confidential information

If a user needs to send confidential information to the outside world, he/she must encrypt the email containing confidential information with encryption software licensed by the IT Department. Encryption is unnecessary for internal emails as they are protected by access control.

10.1.3 Storage of attachments

Users are responsible for saving important attachments that may be used in the future. Attachments cannot be stored in the email system, but stored on the network drive for saving.

10.1.4 Email content

Users' emails shall not include any profane, obscene or derogatory words and expressions.

10.1.5 Use of email system approved by the Company

Users must use approved email (e.g. MSOutlook). Users shall not use their private email address or third-party email address to receive or send any email of Chifeng Gold. In addition, they shall not receive or send any email of Chifeng Gold by using email addresses on the Internet (e.g. Yahoo, and Hotmail, etc.).

10.1.6 Identification of sender

No matter where the email comes from, users must be careful when opening it. All attachments will be scanned by approved antivirus software. Users shall not open emails or attachments from unknown sources.

10.2 Rational use of network

10.2.1 Commercial purpose

The right to use the Internet provided to employees of Chifeng Gold can only be used for business matters of Chifeng Gold.

10.2.2 Reliability of information

Information from the Internet is suspicious and must be checked from other sources. Chifeng Gold shall not trust the identity of a person on the Internet unless the identity of this person can be verified by a digital certificate or digital signature of the IT Department.

10.2.3 Download software

All employees of Chifeng Gold shall not download any unlicensed software from the Internet (8.1.3 Standard application software). It is forbidden to download non-business software such as music, videos and photos. Employees may download files from the Internet, but they must scan for viruses before executing them.

10.2.4 Sending security information

Chifeng Gold shall not transmit sensitive information such as credit card number, telephone number, password or user account number unless such information is encrypted on the Internet.

11.0 System violation reporting

11.1 Users must promptly report the following non-compliance to the IT Manager who will make further investigation and evaluation:

- Serious information vulnerability.
- System violation.
- Lost or stolen electronic data.
- Disclosure of confidential information.

11.2 System violation

11.2.1 An employee violates the system when he/she does not follow the system set forth in the information technology security operating system guidance document.

11.2.2 Impact

11.2.2.1 When an employee violates the system, the General Manager must immediately report such violation to the manager responsible for handling the violation who has the responsibility to correct any system violations immediately.

11.2.2.2 If a violation is not resolved per provisions in 11.2.2.1, the General

Manager will report it to the vice president of operations.

Appendix A: New User Access Request Form & Setup Checklist

Section 1-Request（To be completed by Human Resources)									
Name and Register Number		Hiring Manager's Name		**Employment Type**					
				Permanent	☐				
Position Title		FinanceU8account:	Yes ☐ No ☐	Temporary:	☐				
Dept/Cost Center		Start Date (Mmm/DD/YY)		End Date(Mmm/DD/YY)					
List email Group:(Please pick the appropriate email group)									
All China Staff	☐	All Beijing Staff	☐	All Shanghai Staff	□	All HongKong Staff	☐	All Jilong Mining	☐
All Wulong Mining	☐	All Hanfeng Mining	☐	All Guangyuan	□	Chifeng all Executive	☐	Chifeng all Managers	☐
Chifeng all Superintendents	☐								
Human Resources (HR)									
Name									
Signature									
Date									
Section 2-Request (To be completed by Associate's Department Manager)									
PURCHASING REQUIREMENTS									
The Hiring Manager must submit a Purchase Requisition at least 3 weeks prior to start date for new PC, monitor, and/or non-standard software									
Desktop Laptop	☐ ☐	If YES, then info to be completed by IT	PC inventory# Monitor☐ Keyboard☐						
Comments (Special Hardware Requests etc.):									
Standard Applications									
The hiring manager may specify additional software to be installed. Any additions must be reflected in the Purchase Requisition.									

Windows 10 professional Microsoft Edge Microsoft Office 365(word, excel, PP)	Microsoft Outlook Microsoft Media Player Antivirus Program	Adobe Acrobat Reader WinZip Feishu
Other:		

Section 3-Completion					
TO BE COMPLETED by IT Department					
Email Address：					
Network Setup：					
User Logon ID：					
Password：					
To be completed by IT Manager					
Name		Signature		Date completed	

Appendix B-Major Applications Supporting Financial Process

Business application	Business Department	Administrator
UFIDA U8	Finance Department	Zhao Guangji

Appendix C

Approval Form for Adding and Changing Account Permission of Financial System

<table>
<tr><td>Applicant:</td><td></td><td>User:</td><td></td><td>User’s position:</td><td></td></tr>
<tr><td>Date of application:</td><td></td><td>Start time:</td><td></td><td>User name code:</td><td></td></tr>
<tr><td rowspan="9">Company name:</td><td>☐Headquarters</td><td rowspan="9">Roles:</td><td>☐ Financial Director</td><td colspan="2" rowspan="8">Remarks:</td></tr>
<tr><td>☐Jilong Mining</td><td>☐Chief Accountant</td></tr>
<tr><td>☐ Wulong Mining</td><td>☐ Cost Accountant</td></tr>
<tr><td>☐Tongxing Concentrator</td><td>☐Materials Accountant</td></tr>
<tr><td>☐Hanfeng Mining</td><td>☐ Fixed Assets</td></tr>
<tr><td>☐ Chijin Fengyu</td><td>☐Cash Teller</td></tr>
<tr><td>☐Chijin Geological Prospecting</td><td>☐Audit Accountant</td></tr>
<tr><td></td><td>☐Warehouse Keeper</td><td>Warehouse name:</td><td></td></tr>
<tr><td rowspan="2">Signature of the applicant:</td><td colspan="2">Leader in charge of finance:</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="2">Signature of superior unit:</td><td colspan="2">CFO:</td><td colspan="2">Finance Department:</td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td>System Administrator:</td><td colspan="2"></td><td></td><td></td><td></td></tr>
</table>

Review & approval process:

① Subsidiary application: Financial manager (Applicant) - Leader in charge of finance -Financial manager of superior unit- CFO of superior unit - End;

② Headquarters application: Financial manager (Applicant) - Leader in charge of finance - End

Note: The applicant is the financial manager of the applying unit. It is necessary to fill in the information such as the user’s position and check the company name and the role. If the role is warehouse keeper, the warehouse name shall be given.

1.General Information (For Request User)			
User name:		*User Account:*	
Department:		*Location:*	
Signature By Manager:		*Request Date:*	

2.Access Request (For Request User)		
Fold/File Name:		
Fold/File Full Path:		
Request Description:	*Read Only* □	*Modify* □
Signature By Target file Manager		
Additional Details:		

3.IT Operation (IT USE ONLY)								
Request Permission Level:	**None** □	**Full Control** □	**Modify** □	**Read** □	**List Folder Contents** □	**Read** □	**Write** □	**Special Permissions** □
Additional Details:								
Operated By			Date					

Appendix D – Access & Building Common File Request Form

Appendix E – Account Suspension/Termination Form

1. General Information			
User Name:		*User Account*	
Email:		*Department:*	
Supervisor/Manager:		*Location:*	
Requested By:		*Date Requested:*	
The Mail Is Requested For Keeping For	☐0day ☐5days ☐10days ☐20days ☐30days		

2. Approvals			
Signature of HR Approver：		*Approval Date:*	

3. Account Removal By IT Team					
	User ID	*Deleted*	*Disabled*	*N/A*	*Comments*
Network/AD Account		□	□	□	
OA Account OA		□	□	□	
U8Account		□	□	□	
Feishu Account		□	□	□	
Other		□	□	□	
ITUSEONLY					
Activity Performed By:		*Date:*			

4. Additional Notes	
Special Instructions:	
IT USE ONLY	
Additional Notes/Comments:	