Chifeng Jilong Gold Mining Co., Ltd.

Information Backup and Recovery System

December 2022

1. Purpose

This system is designed to protect electronic data from loss and destruction and, where necessary, to recover the lost date and retain electronic data.

2. Scope

This system applies to all electronic information stored on the network of Chifeng Jilong Gold Mining Co., Ltd. (hereinafter referred to as “Chifeng Gold” or “the Company”).

3. Data backup and recovery

4.1. It must be carried out by IT staff.

4.2. All failed backup files shall be recorded and re-backed up regularly. All failed backups are re-performed to ensure that the data backup is successful, and are checked again at the next backup.

4.3. Tape backup and all other storage media shall be classified and safely stored in the IT Department of Chifeng Beijing Headquarters.

4. Data recovery from backup media

4.1. All files from the backup storage media that are ready to be recovered must be approved by the IT Manager and the authorized data owner before recovery. The IT Manager shall inform all departments affected by the data recovery and explain to them all the links and details to be involved in the process of data recovery.

4.2. Recovery of backup file data must be tested periodically by completing the *Annual Data Recovery Test Form* (Appendix A). All data must be recovered once a year for the following purposes:

4.2.1. To ensure the possibility that all data can be completely recovered, it is necessary to select important systems and test their reliability.

4.2.2. To ensure that all functions of the data backup system can run correctly and smoothly.

4.2.3. The time of data recovery shall not affect commercial operation.

4.3. The IT Manager and the Financial Manager shall sign their manes when confirming the successful recovery of backup data.

4.4. In case of failure in data recovery, it shall be reported to the IT Manager in time for effective review and remedy.

4.5. When performing and monitoring backup, the person performing backup must not conflict with the person monitoring backup.

5. Backup data schedule

5.1. The daily data shall be backed up incrementally every day.

5.2. All the data of one week shall be backed up every week.

5.3. Only the IT Manager or authorized person has the right to establish or modify the data backup schedule.

6. Monitoring of timed tasks

6.1. Timed, regular and automated tasks in servers and applications may not be created without the consent of IT Manager.

6.2. The IT Department will arrange a special person to check the approved timed tasks and ensure that they are running properly.

7. Prevent environmental damage to information resources

7.1. The server workstation shall have proper environmental control, proper temperature and humidity control and robust fire protection facilities.

7.2. Servers shall be placed on a dedicated server rack so as to make good use of space and manage lines.

7.3. Smoke or fire alarm detectors, fire extinguishers (CO2-B) and air conditioner shall be provided in the server workstation to maintain the proper temperature of the server.

7.4. Uninterruptible power supply (UPS) shall be provided in the server workstation in case of power failure.

7.5. The IT Department regularly checks UPS every 7 days.

Appendix A: Annual Data Recovery Test Form

	Test date	*(mm/dd/yy)*

1. System recovery test results	
Backup recovery procedure and recovery media number and name	
Recovery method:	
Recovery data size:	
Recovery data type:	
Time to recover data:	
Is the test successful	*Yes* □ *No* □
If not, please explain the reasons	