File No: EM-IT-MIS.01-04

# Emeren Group Ltd.
# Enterprise IT Management Policy

☐ Level 1 management file First level management document
☒ Secondary management document Secondary management document

| | |
|---|---|
| Preparation Dept: | Internal Control/IT Department. |
| Internal Control Review IC | Chris Wang |
| Approved by the Approval: | Group CEO Guomin Liu |
| Execution | 2023 |

# E-mail management system

## 1. purpose

The purpose of this system is to standardize the operation and management of Emeren Group's email system, ensure the availability, stability, and security of the system, and promote the stable operation of the company.
Scope of application: Emeren Group and all its subsidiaries.

## 2. Definition interpretation

Email is one of the important means of information exchange within and outside the company.
System changes refer to any modifications made to the software and hardware system parameters, database data, or hardware system status of application system programs running in the environment. System changes include email system hardware and software configuration changes, system upgrades, and patch installations.

## 3. Code of responsibility

The IT department is responsible for the daily maintenance of the company's email system to ensure its safe and effective operation, mainly including:
1) Account cycle management (such as application, change, cancellation, etc.).
2) Daily system maintenance (such as system data backup and storage, software maintenance, optimization and upgrading, etc.).
3) Provide training, consultation, and problem-solving services for daily system operation to ensure the effective operation of the system.
4) Strictly comply with the company's information security requirements, ensuring the confidentiality, integrity, and availability of business data.
5) The correction of abnormal data during system operation must strictly follow the system change management procedure.
6) Develop email management systems and operational procedures, supervise all departments to comply, and ensure stable system operation.

## 4.Business departments:

Each business department should strictly comply with the group's email management system. To ensure the security and stability of the system, if any abnormalities or malfunctions are found during system use, the IT department should be consulted in a timely manner.
Except for daily work requirements that meet the audit requirements, strictly abide by the company's confidentiality system, and strictly prohibit sending or forwarding all technical parameters, electronic drawings, personnel information, wages and budgets related to customers, suppliers, finance, engineering drawings, EMC, EPC contracts, etc. through the email system.

## 5. Email management requirements

1) Email account management
Email accounts are managed by the IT department, and account applications, changes, and cancellations must strictly comply with regulations.
2) Account application and change management
When the IT department opens an email account, they will receive a formal on-boarding notice from functional department employees.
3) Account closure management
After receiving a formal employee resignation notice, the IT department should cancel their email in 2

working day of resignation. If business requires, the account should be kept for a period of time and employee approval should be directly submitted to the person in charge of the department or change their email account and password to temporarily resign which is held by the department head.
4) The IT department should obtain a list of departing employees from the Human Resources department at the end of each month and check their email accounts to ensure that they have been cancelled.

**6. E-mail system use and management**
The company has launched an email service with the aim of better promoting internal and external information exchange among employees and improving work efficiency.
1) There is no email delivery unrelated to the job content.
2) Sending confidential company information to external networks via email must be approved by the manager.
3) Sending top secret information to the company via email is strictly prohibited.
4) Sending company information through non company email is strictly prohibited.

**7.Microsoft Office Outlook is the only email client software designated by the company**
Employees should properly manage their personal accounts and passwords and are not allowed to share email addresses with others. If any illegal use of user accounts or security vulnerabilities are found, they should be reported immediately to the IT department.

**8.Prohibit employees from creating and spreading email viruses and spam emails**
Employees are prohibited from sending or forwarding any illegal, reactionary, obscene, maliciously defamatory, insulting, or threatening emails that infringe upon their legitimate rights and interests. Employees are not allowed to use email to promote cults and feudal superstitions, spread rumors, or disrupt company order.

**9. E-mail system change management**
Email system changes should be coordinated by the IT department, and all system changes must be recorded in detail. The Information Technology Department should record the change content, applicant, and executor.
Without authorization, IT email system administrators are not allowed to access or modify the email addresses of other employees in any form.

**10. E-mail system technical support**
If employees encounter email issues, they should contact the IT department.
After receiving a user request, the IT engineer should confirm employee information and resolve the user request within a specified time based on the type of problem. After the IT engineer solves the problem and receives user confirmation, update the request record and close the request.

## Information security code of conduct

**1 Purpose**
This system describes the relevant requirements for IT information security for employees of Emeren Group, in order to enhance security awareness, standardize the use of PC and IT systems, ensure confidentiality, consistency, and availability, and ensure the development of Emeren's business.

**2 Scope of application**
This system is applicable to Emeren Limited and its subsidiaries, as well as other third-party personnel authorized by Emeren to access Emeren's internal IT systems.

**3. Code of responsibility**

The system is implemented by the IT department with the cooperation of all departments.

**4. Management requirements**

**4.1 Client computer management requirements**

1) All PCs that can access Emeren's internal information systems must be official employees of Emeren, who are end users and responsible for terminal security issues.
2) The company computer must be equipped with a compliant operating system account password and BIOS hard drive password.
3) The company computer must be equipped with a screen saver lock automatic activation function and a password that meets the requirements. The maximum standby time for activating the screen saver should be less than 15 minutes.
4) Employees and company emails must be authorized and unauthorized access to company emails is prohibited. Prohibit the use of automatic email forwarding function. If there are specific business requirements, they must be approved by the department head or above management personnel. Do not send or forward emails without approval.
5) Anonymous or unauthorized access to confidential information of others or personal storage devices that store confidential information is prohibited. Individuals with sharing requirements should obtain prior authorization.
6) When the operating system prompts for an upgrade, the system upgrade must be completed within five working days (you can contact your IT engineer for assistance).
7) It is prohibited to use the Emeren network and internet to transmit, download, and browse content unrelated to the company's business.
8) When the operating system prompts for an upgrade, the system upgrade must be completed within five working days (please contact IT for assistance).
9) If it is not possible to lock the workspace to ensure the physical security of the client computer, please ensure the security of the computer when briefly leaving the workstation (for example, manually enabling a password protected screen saver).
When traveling or not working in the office area for a long time, the following regulations must be followed:
A. If possible, it is recommended to carry a computer and handheld devices with you.
B. When taking transportation, it is necessary to carry a computer with you and not put it in your luggage to prevent equipment theft during airport security checks.
C. Do not leave the computer in an unmanned vehicle or unattended indoor or outdoor environment for an extended period of time. If it is necessary to leave it in an unmanned vehicle for a long time, please place it properly to avoid theft.
D. If you need to place your computer outside the office area, place it in a lockable place and then lock it.
10) If traveling with portable storage devices that store Emeren confidential information, such as portable hard drives and USB drives, they must also be properly stored through the above security measures.
11) When replacing or returning a computer, IT desktop support personnel must be contacted to clear the computer data.
12) If the company computer is lost or stolen, you must immediately notify IT and your direct reporting supervisor.

**4.2 Management requirements for handheld mobile devices**

1) If device functions are supported, handheld mobile devices for Emeren services must encrypt their data communications.
2) Please keep the handheld mobile device properly for any loss. If equipment loss occurs, please immediately report to the IT department and the direct reporter, department director, and personnel director.

**4.3 Equipment safety requirements**

If the device is working properly, please set the power on password, lock password, and other functions. The timeout setting should not exceed 15 minutes.
If device functionality is supported, please set up 10 or more illegal data access attempts and automatic data

deletion functions. If the Bluetooth function is enabled, the security function must be set up.

**4.4 Management requirements for portable storage devices**

1) Portable storage devices carrying confidential information (such as CDs, portable hard drives, USB drives) must be marked with information confidentiality labels. The replication, access, modification, deletion, dissemination, and movement of confidential information must be approved by the department head. Approval records must be kept for two years and meet the audit requirements.
2) Storage devices with confidential information must be stored in lockable locations. If confidential information is stolen or lost, the responsible person should immediately report to IT and their immediate supervisor.
3) Storage devices containing confidential information must be reformatted or physically damaged in order to clear data before being discarded.

**4.5 Anti-computer viruses and other malicious codes:**

**4.5.1 The antivirus software specified by Emeren must be installed and run on the client computer.**

1) Real time protection of antivirus software must be enabled, and the virus definition code file must be up-to-date (within one week).
2) Do not use Emeren resources to design and spread computer viruses and other malicious code.
3) If the antivirus software cannot detect the virus, the company should immediately disconnect from the company network and notify IT desktop support personnel to take action.

**4.5.2 Security Firewall**

1) The firewall software specified by Emeren must be installed and running on client computers, and accept appropriate server-side management.
2) The default settings for newly detected networks by the firewall must be trusted or not unknown.
3) When a new program is required to access the network, the firewall must prompt the end user.
4) Deny access from unauthorized systems.
5) Maintain the latest version upgrade of client firewall software.

**4.5.3 File sharing management requirements**

1) Unauthorized access to others' company computers is prohibited.
2) Prohibit providing file sharing services without any read/write permissions and password protection.
3) Anonymous FTP, TFTP, unauthorized HTTP, or other unauthorized network services are not supported on the client computer.
4) Prohibit the installation and use of peer-to-peer file sharing software.

**4.6 Management requirements of software copyright and intellectual property rights**

1) When installing and using any software on client computers, it is necessary to comply with the relevant laws and regulations of the host country and Emeren. The client computer should install software with legal copyright authorization. No employee is allowed to install and use pirated and illegal software on customer computers. Any violation of regulations will be considered as personal behavior, and all consequences (including but not limited to economic losses caused to the company) resulting from this will be borne by the individual.
2) The standard software provided by Emeren is the property of Emeren, and it is only allowed to be installed on office equipment provided by Emeren for employees and authorized third-party personnel.
3) Install only the standard operating system and application software specified by Emeren on the client computer. If the company's business requires the use of commercial software other than standard software, it should be submitted to the IT department for filing and can only be installed and used after obtaining legal copyright authorization.
4) The vast majority of information and software (programs, audio, video, data files, etc.) provided in public places (including the internet) are within the scope of ownership or intellectual property protection.
5) When using this data in Emeren, the following regulations must be followed:

A. Unless the information owner explicitly agrees, such information shall not be used in Emeren.
B. Before using any software, it is necessary to carefully read its license agreement, especially its restrictions. If there are any aspects of Emeren's use that are inconsistent with these regulations, please do not download or use these materials.
C. Ensure compliance with the explicit requirements or restrictions in the license agreement regarding the software used (such as not for commercial purposes, not charging fees to other users or distributors, etc.).
D. If the meaning of other clauses or clauses in the agreement is unclear or in doubt, please contact the Emeren Legal Department before downloading and using these materials to further understand the relevant clauses.
E. If you want to publish Emeren's information in public places or internet, please consult the legal department to ensure that Emeren is the legitimate owner of intellectual property.

**4.7 Account and Password Security Management Requirements**
1) The accounts and passwords of all IT systems (such as operating systems, ERP, OA, etc.) cannot be empty.
2) The password should be at least 8 characters long and should contain both alpha and non alpha characters (numbers, punctuation marks, or special characters), or at least two non alpha characters. Try not to include names, birthdays, sequential numbers such as 666666, 8888888, 111111, 123456, etc.
3) The username cannot be used as part of the password.
4) The password must be changed at least once within 90 days. If the system does not have the function of regularly forcing password changes, employees should fulfill their responsibility of changing passwords in a timely manner.

**4.8 No unauthorized use or attempt of someone else accounts and passwords.**
1) Emeren Confidential information must be marked with information confidentiality, such as electronic documents, E-mail, drawings, and storage equipment. Each department must designate the person responsible for the confidential information to define and control the process for the copying, access, modification, deletion, diffusion, and movement of the confidential information. Confidential information must be encrypted and access rights controlled. Approval records must be kept for two years and shall be able to meet the audit requirements.
2) Any form of disclosure and theft of Emeren's confidential information is prohibited. Any disclosure or theft of confidential information shall be reported to IT desktop support personnel.
3) Confidential information must be encrypted when transmitted on the Internet, public networks, and wireless devices.
4) Prohibit storing or processing confidential information on a system not controlled by Emeren. When using OA, MSD, corporate email, online banking, and other corporate accounts, do not use public computers (Internet cafes, hotel computers, public networks, etc.) for login operation。
5) It is forbidden to enter Emeren confidential information (such as websites and forums providing translation services) on websites that are not controlled by Emeren.
6) When the Emeren confidential information, personal or sensitive information is stored on the portable storage device, the device marking information must be kept confidential (see 4.3 for details).
7) Security measures must be taken to control the access to the Emeren Confidential information stored on the computer system (website, shared database, etc.).
8) Unauthorized access of any form to Emeren confidential information and procedures is prohibited. Please pay attention to security protection to avoid losses caused by data leakage and account theft, timely identify and delete phishing emails, prevent the sender, and do not click on the attachments.

When printing the confidential information of the Emeren, the following measures must be taken:
Secret information must be printed on a controlled printer.
When printing confidential information, it must be approved by the relevant responsible person.
If confidential information is printed in an open internal area, the printed document must be removed within 10 minutes.

9) A secure conference call system must be used for any discussion or presentation of confidential information. Before the call, confirm that all participants are authorized to attend.

**4.9 Management requirements of the work area**
1) For public offices, please lock their laptops and Emeren confidential information when employees leave their desks.
2) The confidential information of Emeren is not authorized to be discussed during open meetings with third-party companies or organizations.
3) External personnel are not allowed to enter the office without authorization.
4) Unauthorized access to non-business areas or areas with access restrictions.
5) Leave messages with confidential information on non-Emeren voicemail or fax machines.

**4.10 Security management requirements for using Emeren internal network resources**
1)Without the explicit authorization of the Emeren IT department, it is forbidden to add any network equipment to expand the network infrastructure of Emeren, such as switch, network bridge, router, Hub, Modem, wireless base station, etc.
2) Third-party personnel to access and use Emeren's internal network resources must strictly comply with the security requirements of third-party personnel to access Emeren's internal IT system (see appendix for details).
**4.11 Security Event Report**
If you find information security problems or hidden dangers in yourself or other personnel, you should immediately report to the IT department and the Compliance Director, provide relevant information, and actively cooperate with the follow-up investigation.

## Online behavior management system

**1 Purpose**
This system describes the company's management requirements for internet behavior, ensuring employee work efficiency and effective utilization of network resources through the management of employee network access content and time.

**2 Scope of application**
This system is based on the Management Measures for Computer Information Network Protection, and other relevant regulations and policies are formulated according to the specific situation of the company. Applicable to Emeren Group and its subsidiaries.

**3. Code of responsibility**
This system is managed by the IT Department, Internal Control Department, and HR Department, and implemented with the cooperation of all relevant departments.

**4. Internet access behavior management requirements**
4.1 Network Information Access and Management Requirements
1) It is prohibited to install and use instant messaging tools that are not designated by the company. Specific business requirements require approval from department directors and HR directors.
2) It is prohibited to use enterprise networks to access BBS, blogs, and online games, such as simulation games, streaming media, large-scale online games, etc.
3) It is prohibited to use the company's network to publish, browse or disseminate all entertainment, shopping, reactionary, cult, pornography, gambling, making friends, securities, violence and other network

information unrelated to work.
4) It is prohibited to watch online videos such as YouTube, Bilibili, and iQiyi.
5) It is prohibited to input company confidential information in any form on the public internet, such as online translation websites, libraries, forums, etc.
6) The Information Technology Department restricts and monitors network access through internet access behavior monitoring software. For violations of company regulations, the IT department should follow up and report the results to the department head of the employee. If the violation affects, IT should also notify relevant departments (such as human resources or legal).
8) The IT department should conduct regular audits of network access logs and track any violations.

**4.2 Requirements for Network Management**
1) Prohibit the installation and use of P2P and other upload and download software that affects network speed, such as BT, Thunder, and Netdisk.
2) The IT department should allocate network bandwidth to meet work requirements based on the business needs of each department. If bandwidth needs to be increased, approval from department heads and IT engineers is required.
3) For abnormal changes in network traffic, the IT department should promptly track and investigate, and report the results to the relevant department heads.
4) The IT department should conduct daily monitoring and statistics of network traffic, and adjust bandwidth based on the actual traffic of each department to ensure the effective utilization of network resources.
5) All employees are not allowed to engage in online activities unrelated to work during working hours.

**4.3 Management requirements of Internet access behavior system**
Administrator account and password management
1) The account management of super administrators and log administrators should comply with the Emeren Group IT System Account Usage Management Procedure.
2) The administrator account used for daily system maintenance should be managed and used by information security engineers, and comply with the Emeren Group Code of Conduct.

## Network security measures

1.Payment alteration processes(In MSD and OA): We should ensure it has a process to confirm with the organisations when they request their bank details are changed. Likewise, we should communicate to organisations that they would never request their bank details changed, and to confirm via phone call. Minimize the use of email payment requests unless in very urgent situations.

2. User training: Implement or review formal training and awareness for employees covering cyber security and email phishing. Fundamentals of cyber-security should be covered and assessed. Specific material on how to identify and report malicious and fraudulent websites should be included. A formal process should be implemented for reporting suspicious emails to the IT team. This should inform containment and investigation of potential incidents, as well as continually improve anti-phishing controls by informing domain blacklisting, file type blocking and other in-house measures. Any potential cyber security incidents should be reported in a timely manner so that time-sensitive logs containing evidence that may be required for any investigations can be captured.

3. Mail filtering: Update existing mail filtering technology to improve rates of spam and malicious email detection and blocking. Strengthen gateways with additional measures in a layered approach to filtering.

4. MFA: MFA should be enabled and enforced on accounts and all other applicable services, such as third-

party hosting providers and remote access methods. As a priority, ensure privileged accounts are protected with MFA.

5. Access control and credential use. Passwords should be long, complex and unique to each user account. Consider using a passphrase featuring numbers, characters and one misspelled word. When reset, passwords should be entirely changed and not simply modified. Mult-factor authentication (MFA) should be enabled and enforced on email accounts and all other applicable services.

6. Enable number-matching and additional context in MFA applications. Do not allow user consent for applications accessing Microsoft 365 and Azure (this may require users to receive admin approval when using new applications). Consider if conditional access policies can be put in place and are appropriate, e.g. sign-ins can only be received from set IP address if static or device. Consider using FIDO2 hardware-based MFA for key users.

7. Technical controls. We should conduct a security review with its IT provider to ensure that relevant security logging is enabled to a suitable standard. This is to enable post-incident investigations and increase the likelihood that future incidents can be investigated fully if they occur.

8. In operation-Legacy protocols such as IMAP should be disabled unless they are required for business operations. Update existing mail filtering technology to improve rates of spam and malicious email detection and blocking. Strengthen gateways with additional measures in a layered approach to filtering. Macros should be blocked as standard.

9. Now Microsoft's default protection has been enabled-Centrally managed antivirus or endpoint protection should be enforced on all corporate devices to detect and block malicious infections resulting from email attachments.

10.All corporate devices and systems should be regularly patched and kept up to date.

## System master document, data maintenance process

**1. Supplier Master File**
1.1 The establishment and modification of the main documents of the supplier shall be requested by the corresponding user and the ERP addition/change application form shall be filled out and submitted for OA approval. The content of the supplier master file includes the supplier name, supplier type (internal and external), tax group, country, and language.

**2. Customer Master File**
2.1 The construction/modification of customer master files requires corresponding user applications and the completion of ERP new/change application forms for OA approval.
2.2 The content of the main customer documents includes the customer name, customer type (internal and external), tax group, country, and language.

**3. Project Master File**
3.1 The construction/modification of the main project documents requires corresponding users to apply and fill out the ERP new/change application form, and submit it for OA approval.
3.2 The content of the main project documents includes: project name, project type (investment, cost), scale (installed capacity), country and project company (entity ID)

**4. Bank Accounts Master File**
4.1 The creation/modification of main bank documents requires the corresponding user to apply and fill out the ERP addition/change application form, and submit it for OA approval.
4.2 The content of the bank master file includes the bank name, bank account number, main account, currency, and project company (entity ID).

**5. New company Master file**
5.1 The creation/modification of new company documents requires corresponding user applications and the completion of the ERP addition/change application form, which should be submitted for OA approval.
5.2 The content of the bank master file includes the new company name and account set.

**6. Record-keeping**
All main document modification requests shall be continuously numbered, saved, and updated to the OA and MSD systems by the administrator.

**7. Record retention**
All original records of this document should be archived by the IT department.

**8. Duties of the IT Department**
1) Responsible for the revision, training, promotion, management, and implementation of this system.
2) Ensure the effective operation of the Internet access behavior management system.
3) Regularly test the implementation of this system and report the results.
4) Track violations and cooperate with relevant departments to handle them.
5) IT Desktop Support Engineer:Null - chong.deng@emeren.com provides relevant technical support.

**9. Validity of the documents**
This management system is approved by the CEO's.It shall be implemented from the date of approval.

**10. Punishment measures**
Those who violate the above regulations but do not affect the company's system or the office of others will be given a warning and punishment, and the punishment will be reported within an appropriate range. If affected, fines may be imposed based on the severity of the situation, and even labor relations may be terminated.