CYBER SECURITY POLICY

OGPL/HR/Cyber Security Policy/2022 **1st April 2022**

Policy brief & purpose:-

Orient Green Power Company Limited and its subsidiaries cyber security policy outlines the guidelines for preserving the security of our data and technology infrastructure.

We are conscious that the more we rely on technology to collect, store and manage information, the more vulnerable, we become to severe security breaches. Human errors, hacker attacks and system malfunctions could adversely impact the business and may jeopardize our company's reputation.

To mitigate this risk of security breach, we have put in place security measures. We have also prepared instructions that may help mitigate security risks. We have outlined them in this policy.

Scope

This policy applies to all our employees and anyone who has permanent or temporary access to our systems and hardware.

Policy elements :

Confidential data

Confidential data are secret and valuable

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we have outlined instructions on how to avoid security breaches.

Protect personal and company devices

When employees use their digital_devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

Contd—2

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive company-issued equipment they will receive instructions for:

- Accessing company Email account
- Connecting to our Financial Application securely
- Archiving the data when needed.

They should follow instructions to protect their devices and refer to our System support Engineer if they have any questions.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can refer to our System support Engineer.

Contd-3

Data Security

To ensure the company related data's (like Email, Financial application data, Documents related to the transaction) are in safe and secure and to make sure its preserved even in the event of disaster, we have hosted these applications in the secured cloud environment. Automated daily backup procedure is in place and it will be retained for the last 7 days of daily copies in different environment. Once in a year we will be performing the data restoration test and the logs will be submitted at the time of system audit which will be conducted every financial year.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records and other details) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our System support Engineer for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Contd—4

Our System support Engineer need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our System support Engineer must investigate promptly, resolve the issue with the help of supporting team and send a companywide alert when necessary.

Our System support Engineers are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR/IT Department.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

Our System support Engineer would:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

Remote employees

Remote_employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our System support Engineer

Contd—5

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We will issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
  We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

FOR ORIENT GREEN POWER COMPANY LIMITED,

G.HARIKRISHNAN
HEAD HR & ADMIN