Cyber Security Policy for End User

1.1 Introduction

IRM Energy Limited's ("IRMEL" / "Company" / "we") cyber security policy outlines the guidelines and provisions for preserving the security of Company's data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we are to severe security breaches. Human errors, hacking attacks and system malfunctions could cause great financial damage and may jeopardize the company's reputation.

For this reason, the Company has implemented a number of security measures. The Company has also prepared instructions that may help mitigate security risks. The measures are outlined in this policy.

Purpose of the Policy

This Information Security Policy/Cyber Security Policy ("Policy") expresses IRMEL's commitment to effectively and efficiently manage information security risks in compliance with applicable regulations wherever it conducts its business.

This Policy is the foundation for all information security activities. It focuses not only on the technology for the storage, processing, and transmission of information, but also on administrative and operational practices for the protection of all information, data, files, and processing resources owned by IRMEL

It is the intent of this Policy to facilitate the exchange of information and computing resources while balancing the need for protecting information with the cost of implementation.

This Policy is the property of IRMEL. It is intended for distribution to all employees and users of information systems at IRMEL locations.

1.2 Scope

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

1.3 Policy Elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished price sensitive information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

All employees are obliged to protect this data. In this policy, we will give our employees 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 their company-issued computer, tablets and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Install and upgrade a corporate antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems periodically.

- 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.

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 IT Support.

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 month.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary.
- Share confidential data over the company network/ system and not over public network/Wi-Fi 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
- Limit use of external storage drives, only company's authorized device must be used.
- Use Google Drive or Microsoft /OneDrive for transfer of bulk data.

IT Department needs 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. IT Department must investigate promptly, resolve the issue and send a companywide alert when necessary.

IT team is 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.

We also expect our employees to comply with our internet usage policy.

General and Internet Usage

Employees and contractors shall not, under any circumstances, use IRMEL computing devices or information systems to:

- Engage in any activity that is illegal or violates the rights of any person.
- Download or install software of any type on IRMEL computing devices without authorization.
- Copy or distribute any copyrighted material without authorization.
- Access the personal information of others without authorization, except as part of the employee's or associate's assigned duties.
- Make any claims on behalf of IRMEL unless authorized to do so.
- Associate IRMEL activity that would harm the reputation of the organization.
- Visit websites exhibiting sexually explicit material, gambling sites or sites related to illegal activities.
- Visit websites that encourage discrimination or the violation of the rights of any group or individual, except in the course of authorized research.
- Visit websites which share music or other files on a peer-to-peer basis, or otherwise share content in violation of copyright laws.
- Engage in any activity that interferes with the ability of another organization or individual to conduct computing activities (e.g. denial of service attacks).
- Provide information about IRMEL or its employees, clients, customers, patients, or associates to any outside party, unless explicitly authorized to do so.
- Post comments or other information to social networking sites or blogs on behalf of, or using the name of the organization, unless explicitly authorized to do so.

IT support/team should:

- 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 IT Dept.