Prepared by:		Reviewed & Approved by:
Dastan Ong IT Application Developer		Teh Huat Chooi Chief Technology Officer

INFORMATION SECURITY POLICY

Version 01

1 Apr 2022

STRICTLY CONFIDENTIAL

Revision History

Date	Version	Description
2021/06/01	00	Initial creation of Information Security Policy document.
2022/04/01	01	Update Enforcement section details.

Table of Contents

1.0 Introduction

While MY CO2 Group of Companies (hereinafter referred to as "***the Company***") desires to provide a reasonable level of freedom and privacy, all Employee should be aware that all equipment, network infrastructures and software applications are the property of the Company and therefore are for official use only. All data residing on the Company's owned equipment and/or IT Assets are also the property of the Company and therefore, should be treated as such, and protected from unauthorized access. In the Company, we are committed to uphold and advocate the highest ethical standards and principles of good corporate governance and compliance. Accordingly, the Company requires all Employee to strictly adhere to this policy. Any breach of this policy will be referred to Head of Department who will review the breach and determine adequate consequences, which includes but not limited to confiscation of the devices and/or termination of employment and/or other penalties in accordance to the laws of the country.

1.1 Overview

Information Security Policy is a set of rules and processes for all individuals that work with IT assets and resources which ensure individuals follow the security protocols and procedures to protect data confidentiality, integrity and availability. The Company recognizes the need for its members, employees, and visitors to have access to the information they require in order to carry out their work and recognizes the role of information security in enabling this.

1.2 Purpose & Scope

This Policy seeks to enhance corporate governance and to foster an environment to support integrity and ethical behaviour usage, security and maintenance of the IT assets and resources within the Company.

While this Policy is not a comprehensive guide that covers every usage, maintenance and security of the information technology infrastructure of the Company, Employee shall refer to his Head of Department or the Company's Head of Human Resources Department for clarification or guidance in event of doubt or ambiguity.

1.3 Audience

This Policy applies to all Office Bearers, Employee and IT Department of the Company who may have access to the information technology assets and resources from time to time.

1.4 Objective

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

2.0 Definitions

1) **IT** – Information Technology
2) **Confidentiality** – Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
3) **Integrity** – Property of accuracy and completeness
4) **Availability** – Property of being accessible and usable upon demand by an authorized entity
5) **Associated External Parties** – refers to all associated external parties acting on behalf of or for the Company whom has, or plans to establish, some form of business relationship, including but not limited to, agents, contractors, consultants, suppliers, service providers, associate companies, business partners and joint venture partners or entities.
6) **CTO –** Chief Technology Officer
7) **Confidential Data** – including but not limited to unpublished financial information, data of our Associated External Parties, patents, formulas or new technologies, existing and prospective customer lists**.**
8) **Employee** – means all employees of the Company, including full time or permanent employees, part time employees, contract employees, employees on probation, trainees and interns, employees on secondment and personnel on fixed-term contracts.
9) **HOD** – means the Heads of Department or division heads i.e. Manager
10) **HRD** – means Human Resource Department of the Company
11) **Immediate Superior** – means the Assistant Managers, Supervisors, Team/Shift Leaders and Supervisory level staff.
12) **IT Assets** – means any technological device belonging to the Company that is capable of retaining data, including but not limited to desktop, laptop, point-of-sale computers, mobile devices, peripherals, servers, internet, software/hardware, as well as the programs and data therein contained
13) **IT Department** – means the person or team who are responsible to overseeing the installation and maintenance of computer network systems and software/hardware within the Company.
14) **Material** – in relation to shareholding
15) **MY CO2 Group of Companies** – refers to MY CO2 SDN BHD and all its subsidiaries and associated companies operating now and in future
16) **Office Bearer** – means the directors and the management of the Company
17) **Social Media** – means variety of online communities like blogs, social networks, chat rooms and forums including but not limited to Facebook, Twitter and Instagram

3.0 Policy

Information Security Policy establish formalized rules to ensure that the company has a series of controls around and focus on the three principles: Confidentiality, Integrity and Availability.

3.1 Confidentiality, Integrity & Availability

3.1.1 Confidentiality

Confidentiality of all information assets (information is not disclosed to unauthorized persons through deliberate or careless action). Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The unauthorized disclosure of information could have a limited adverse effect on organizational operations, organizational assets, or individuals.

3.1.2 Integrity

Integrity of all business processes, information assets, and supporting IT assets and processes, through protection from unauthorized modification, guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The unauthorized modification or destruction of information could have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

3.1.3 Availability

Availability of all business processes, information assets, and supporting IT assets and processes to authorized users when needed, ensuring timely and reliable access to and use of information. The disruption of access to, or use of, information or an information system could have a serious adverse effect on organizational operations, organizational assets, or individuals.

3.2 Internet Usage

In the Company, we do not restrict our Employee's access to websites of their choice, but we expect our Employee to exercise good judgement and remain productive at work while using the internet. Any use of our network and connection must follow our confidentiality and data protection policy. All Employee is advised to use of the Company' internet connection for the following reasons:

- To complete their job duties.
- To seek information to improve their work.

3.2.1 Our Employee Should :

- Keep their passwords secret at all times
- Log into their corporate accounts only from safe devices
- Use strong passwords to log into work-related websites and services
- Be careful when downloading and opening/executing files and software. If they're unsure if the file is safe, they should consult HOD.

3.2.2 Our Employee Should Not :

- Download or upload obscene, offensive or illegal material
- Send confidential information to unauthorized recipients
- Invade another person's privacy and sensitive information
- Download or upload movies, music and other copyrighted material and software
- Visit potentially dangerous websites that can compromise the safety of our network and computers
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more

3.2.3 Please be advised :

- The Company may install anti-virus and disk encryption software on the Company computers. Employee may not deactivate or configure settings and firewalls without managerial approval.
- We won't assume any responsibility if Employee devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate Employee use.

3.3 Email Usage

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment. The Employee shall keep in mind that the Company owns any communication sent via email or that is stored on the Company's IT Assets. Management and other authorized staff have the right to access any material in your email or on the Company's IT Assets at any time.

3.3.1 Corporate Email Address

The Employee may be assigned a corporate email address, i.e. yourname@myco2.com.my. Such Employee shall only be allowed to use their corporate email as follows :

- For work-related purposes.
- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

3.3.2 Employee should not use their corporate email to :

- Send or receive personal e-mails.
- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Register for a competitor's services unless authorized.
- Send profanity, ethnic slurs, insulting, sexual harassment or discriminatory messages and content.
- Intentionally spam other people's emails, including their co-workers.

3.3.3 E-mails carrying Malware or Phishing attempts :

- Avoid opening attachments unless you are certain of the sender's identity or it is an attachment you specifically requested the sender to mail to you or you are familiar with the file format and know that it cannot possibly contain any destructive programming (e.g. Adobe Acrobat PDF files).
- Avoid opening on links when content is not adequately explained (e.g. "Watch this video, it's amazing").
- Be aware that Microsoft Word (***.doc***) and Excel (***.xls***) file can contain harmful programs called *macros*. Even if such documents appear to come from a legitimate source, be aware that they could have been mailed without the sender's knowledge.
- Be careful of files with the extension ***.zip*** or ***.exe***. These are almost always with viruses.
- Be suspicious of clickbait titles (e.g. offering prizes, advice).
- Check email and names of unknown senders to ensure they are legitimate.
- Be suspicious of any e-mail that appears to be from a bank or credit company asking you to go on line to confirm personal account information.

3.4 Cyber Security

Everyone, from our Employee to our Associated External Parties, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize the Company' reputation. For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks.

3.4.1 Protect personal and the company devices and it assets

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure that the Employee do not leave their devices exposed or unattended.
- Log into the Company accounts and systems through secure and private networks only.
- Avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

3.4.2 Transfer data securely

Transferring data introduces security risk. Employee must :

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request Employee to ask our IT Department 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.

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

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HOD.

- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in the Company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on the Company equipment.
- Avoid accessing suspicious websites.
- Report scams, privacy breaches and hacking attempts.
- Report perceived attacks, suspicious emails or phishing attempts as soon as possible to our IT Department as they need to know about scams, breaches and malware so they can better protect our infrastructure.

3.4.4 To be advised :

- All relevant data is to be backed-up. It is the responsibility of the Employee to ensure that data back-ups are conducted by the end of the day and the backed-up data is kept in the cloud prepared by the Company.
- All technology that has internet access must have anti-virus software installed. It is the responsibility of the IT Department to install all anti-virus software and ensure that this software remains up to date on all technology used by the Company.
- All information used within the Company is to adhere to the privacy laws and the Company confidentiality requirements.

4.0 Responsibility

The Company shall ensure that all activities required to implement, maintain and review this policy are performed. All personnel must comply with this policy statement and its related security responsibilities defined in the information security policies and procedures that support the corporate information security policy. All personnel have a responsibility for reporting security incidents and identified weaknesses, and to contribute to the protection of business processes, information assets, and resources of the Company.

5.0 Enforcement

The Company holds the right to monitor the compliance of its personnel to this policy. Manager and staff of the Company, all full-time, part-time employees and temporary employees, who fail to comply with this policy, may be subjected to appropriate disciplinary actions.

6.0 Review and Revision

This policy statement is owned by the Board of Directors of the Company who has delegated this task to the CTO. This policy shall be revised by the CTO and IT Executive, decides to do so. Information Security Policy review or revision shall consist of the following members (as approved by CEO) : CTO and IT Executive.