SANWA

Issued on 1st January 2019

INFORMATION SECURITY POLICY

I. WORKSTATION SECURITY

Protecting your workstation area - specifically your desktop computer and other supporting devices - is an important duty all employees should take very seriously.

II. PURPOSE

The purpose of this policy is to:

a. Set out SANWA's principles as well as the responsibilities of those working for us or associated with us to ensure proper Information Security

b. Provide information and guidance to those working for us on how to recognize and deal with these issues

In this policy the use of the terms "we", "our", and "us" refer to SANWA

It is important that you read, understand, and act in accordance with this policy

III. TO WHOM THIS POLICY APPLIES?

The policies apply to all individuals working at all level and grades, including Senior Managers, Officers, Directors, Employee (whether permanent or contract), Consultants, Contractors, Seconded Staff, Home Workers, Casual Workers and Agency Staff, Agents, Channel Partners or any-other person associated with us, or any of subsidiaries or their employees, whether located (collectively referred to as "**Workers**" in this policy)

IV. PRACTICES

With regards to the usage of company Information system including devices it is important to follow these rules:

4.1 **To use primarily for work purposes only.**

4.2 **You are not allowed to install any unapproved software.**

Your workstation has also been configured for providing you the necessary tools in performing daily roles and responsibilities, which means no additional software is needed

4.3 **Use caution with email**. Be careful when opening emails from unknown parties, especially attachments. If it looks suspicious, do not open the email under any circumstances.

4.4 **Handle privileged information with care.** From emails containing sensitive information to hard copy documents for contracts or any other type of confidential data, treat it with the utmost care and professionalism, making every effort to protect its confidentiality and integrity.

4.5 **Report security issues immediately.** Remember, if you see something, say something – and immediately. You have a responsibility for helping protect the organization, which means being aware of your surroundings and reporting suspicious activity to authorized personnel – immediately

4.6 **Shut down and protect your workstation.** When leaving your workstation area at the end of each day, make sure to completely shut down and turn off all computers and related devices. Additionally, pickup and store any documents, electronic media, or any business and/or professional items that should not be left unattended

4.7 **Keep a watchful eye.** Don't ever leave your laptop unattended in any public venue or location not considered safe.

V. MANAGEMENT EFFORT

5.1 Conducting Security Awareness Program at least once a year to workers who use/handle critical information.

5.2 Annual Internal Auditing for Information Security breaches.

VI. RESPONSIBILITIES TO WHOM THESE POLICIES APPLY

6.1 You must ensure that you read & understand this policy.

6.2 The prevention, detection and reporting of any offense are the responsibility of all those working for us or under our control. All Workers are required to avoid any activity that might lead to, or suggest, a breach of these policies.

6.3 You must notify your manager/Compliance Manager as soon as possible if you believe or suspect that a conflict with any of these policies has occurred, or may occur in the future.

6.4 Any employee who breaches any of these policies may face disciplinary action, which could result in dismissal for gross misconduct.

6.5 We reserve our right to terminate our contractual relationship with other parties if they breach this policy.

VII. HOW TO RAISE A CONCERN/WHISTLEBLOWING

You are encouraged and shall be awarded for **raising concerns** about any issue or suspicion of malpractice at the earliest possible stage.
If you are unsure whether a particular act constitutes an offense, or if you have any other queries, these should be raised with our Departmental Head or directing to the Compliance Manager (MIS and HR Department).

7.1 Your identity would be kept confidential. There would be no identity disclosure without your personal agreement and acknowledgment. Your security will also be our top priority.

7.2 Hotline number to report the case is 0811777148, ensure that you have written your complete name, badge number & feedbacks with some evidence. The more complete information you supply us, the most likely the investigation is going to be effective and efficient.

7.3 Ethics Committee shall take action immediately within one week of the report and do prompt investigation, proper

reporting and acknowledgment by Director. The whole process shall not take longer than 6 months except if the impending is caused by External Parties. You would be notified of the on-going process.

7.4 Whistleblower who makes a report which is not done in good faith (intentional false accusation) or the offender of Code of Conduct shall be put into disciplinary actions or even dismissal from employment or partnership for serious offence.

7.5 Criminal offence will be reported to the law enforcement and resulted in automatic dismissal from employment or partnership.

VIII. MONITORING AND REVIEW

8.1 The Compliance Manager will monitor the effectiveness and review the implementation of this policy, considering its suitability, adequacy and effectiveness. Improvements identified will be made as soon as possible.

8.2 All Workers are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.

8.3 Workers are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the Compliance Manager.

8.4 SANWA reserves the right to vary and/or amend the terms of this policy from time to time at its absolute discretion.

Signed and Approved by

Steven Lim
Executive Director

SANWA

----------YOUR DECLARATION FORM----------

I/We are obliged to obey this policy and SANWA reserves the right to terminate the employment/partnership in case we are proved to be breaching SANWA Code of Conducts

DATE : 05 JANUARY 2019

NAME : SANDI MU'MIN

DEPARTMENT/COMPANY : HRD

SIGNATURE & STAMP :

Please submit this form to SANWA HR DEPARTMENT