IT DEPARTMENT

INFORMATION SECURITY RULES AND GUIDELINES

Title:	**Information Security Rules and Guidelines**	
Version:	0.17	
Company(ies):	Nippon Sanso (Thailand) Co., Ltd.	
Owner:	President	
Reviewed by:	South-East Asia Information Task Force members	
Reviewed and Approved by:	Shunichi Watanabe, NSHD IT	
Approved/Ratified by [name of subsidiary board of directors]:	Dr. Suwan Runggeratigul , President	Date of
Issued on:		
Effective from:		
Review date and responsibility:	To be initiated annually by the Information Security Coordinator in discuss with the President.	

TABLE OF CONTENTS

BACKGROUND

This Information Security Rules and Guidelines (hereafter this “**Policy**”) contains rules, policies and general guidelines to guide Users to an efficient, effective and secured use of the computer system of [name of company] (the “Company”) as part of the Information and Communications Technology (ICT) program of the Company. These guidelines are being initiated by the [IT department and approved by the ISD Committee on Computerization] in accordance with the vision and mission of the Company.

1. PURPOSE AND OBJECTIVES

This Policy aims to provide rules and general guidelines to all users/employees of the Company in using the Information Technology (IT) facilities and resources of the Company.

This Policy serves to safeguard three main objectives:

1.1. Confidentiality: Only individuals with authorization can access the Company’s data and information assets and these individuals must not disclose the Company’s data and information assets to others unless authorized.

1.2. Integrity: Data and information must be kept intact, complete and accurate, and IT systems must be kept operational.

1.3. Availability: Authorized users should be able to access information or systems when needed.

2. GENERAL POLICY STATEMENT

The use of IT facilities and computer resources provided by the Company entails responsibility to use these resources in an efficient, ethical, and lawful manner consistent with the mission and vision of the Company. To this end, every user must use such facilities and computer resources in a responsible, professional, and ethical manner and within legal and proper boundaries.

3. SCOPE AND APPLICATION

This Policy shall apply to all full-time, part-time, permanent and temporary personnel employed by, or contracted by the Company, its agencies and offices, including trainees, freelance workers, contract staff, interns and staff seconded from affiliated companies to the Company, management members and directors of the Company, who are authorized to use IT Facilities and Resources (defined hereafter).

This Policy covers the proper use of IT Facilities and Resources.

For purposes of implementing this Policy, any other equipment, computer unit, or external network, when attached to, or used to access and/or interact with any component of the IT Facilities and Resources, shall also be considered part of the IT Facilities and Resources.

The application of this Policy is not limited to existing infrastructure but includes future purchases of IT Facilities and Resources by the Company.

4. DEFINITION OF TERMS

The definition of terms herein provided may be updated from time to time to include new equipment and services as well as new perspectives and developments in the use of IT Facilities and Resources.

For purposes of this Policy, the following terms and phrases shall be understood as follows:

Access - means to connect to a computer system or server that enables one to get online and to browse, retrieve data, and communicate electronically through an Internet service provider (ISP) via a modem or through Network such as an office Local Area Network (LAN).

Authorized Users - refers to all employees, consultants, temporary workers, and other persons authorized by the Company as follows:

- persons who have been specifically authorized by the Company to access and use a particular computer or network resource which are not generally available to Users;
- individuals authorized to connect to a public information service including but not limited to external Wi-Fi service and external information service providers.

Electronic Mail (E-mail) - refers to electronically transmitted mail.

IT Facilities and Resources - include but are not limited to the following items which are used, authorized, controlled and/or operated by the Company: all IT equipment, software, data in all formats, accessories, networking facilities, and services, whether central or remote, including information retrieval services for the general public such as web browsing through the worldwide web (www) and file transfer (upload/download), and the items listed in 5.1 below.

Internet - refers to a system of linked computer Networks, global in scope, that facilitates data communication services such as remote login, file transfer, electronic mail, and news/groups. The Internet is a way of connecting existing computer Networks that greatly extends the reach of each participating system.

Local Area Network (LAN) - refers to a network that connects computers in a small pre-determined area like a room, a building, or a set of buildings. LANs can also be connected to each other via telephone lines, and radio waves. Workstations and personal computers in an Office are commonly connected to each other with a LAN. These allow them to send/receive files and/or have access to the files and data. Each computer connected to a LAN is called a **node.**

Network - refers to a communications system that links two or more computers. It can be as simple as a cable strung between two computers a few feet apart or as complex as hundreds of thousands of computers around the world linked through fiber optic cables, phone lines and satellites or other electronic means.

Official Business - refers to usage in the performance of work-related duties and/or officially authorized activities.

Personal Files - refer to information that a User or the Company would reasonably consider as private. These include the contents of electronic mailboxes, private file storage areas of individual Users, and information stored in other areas that are not public, even if no measure has been taken to protect such information.

Removable media refers to storage media such as a USB flash drive, USB external hard drive, and DVD that can be used to record and save electronic information of a company, and be taken to an arbitrary place to have its data transferred and copied to any personal computer or smart device**.**

Smart device refers to a smartphone or tablet terminal.

Software Applications – refers to software programmes and include the following:

- System applications such as operating systems
- Office applications such as Microsoft Office, Desktop Publishing (such as AutoCaD and Photoshop.)
- Application software such as ERP system

Users – refers to privileged Users who have been given the appropriate level of Access to IT Facilities and Resources and includes Authorized Users.

User Account - refers to a unique identifier which may consist of an account name and a password. This allows the User to access IT Facilities and Resources either through a local area Network (LAN) or the Internet.

Unauthorized Software – refers to any application software installed in the workstation without the permission of the IT department. Application software includes Operating Systems, Office applications, Games, Desktop Publishing (such as AutoCaD and Photoshop), and other software that is unlicensed.

5. IT FACILITY AND RESOURCES SECURITY MANAGEMENT UNDER THE IT DEPARTMENT

The authority and responsibility to install, upgrade or modify any hardware or software rests solely on the IT department and its personnel duly authorized by the head of the IT department.

5.1 The IT Facilities and Resources

The IT Facilities and Resources include but are not limited to the following:

5.1.1. all cabling used to carry voice and data;
5.1.2. all devices to control the flow of voice and data communication, such as hubs, routers, firewalls, switches, and the like;
5.1.3. monitors, storage devices, modems, network cards, memory chips, keyboard, cables and accessories;
5.1.4. all computer software including applications, utilities, tools, and databases; and
5.1.5. all output devices including printers, fax machines, CD writers and similar devices or equipment.

5.2 Responsibilities

The IT department shall have the following duties and responsibilities in implementing these policies:

5.2.1 **Software Upgrades.** The following are considered modifications: installing patches provided by the software supplier or downloaded from the Internet; installing anti-virus; installing new versions of the operating system or any Office applications, e.g., word-processing or spreadsheet applications.

5.2.2 **Systems Inspection and Deletions.** The IT department or its authorized personnel may delete files or software that are unauthorized, provided that this deletion or modification is done in the presence of the User or his/her immediate supervisor.

5.2.3 **Hardware Maintenance.** The IT department or its authorized personnel is the only authorized entity to inspect any ICT equipment. Equipment, software or services under warranty shall not be altered or inspected by unauthorized personnel.

5.2.4 **Equipment Movements.** The IT department or its authorized personnel is the only entity permitted to authorize the movement and/or move and transport equipment from one location to another, including mobile computers such as notebooks, laptops and wireless user devices. Furthermore, the IT department and its personnel is the only authorized department to assign facilities to Users.

5.2.5 **Authority to Secure Equipment and Services.** The IT department or any its authorised personnel shall have the responsibility to maintain security of Internet resources against intrusion and destruction. It is tasked to research security and disaster recovery matters to maintain a high degree of reliability of the systems.

5.2.6 **Purchase Recommendations.** The IT department or its authorized personnel shall have the responsibility to reject or recommend any ICT project. Rejection of the project includes giving options for a better yet cost-effective solution.

5.3 Levels of Security

The IT department and its managerial staff have the sole authority to initiate or modify the level of user accessibilities for both Software Application and Network resources in accordance with the following policies:

5.3.1 Department Heads will determine the level of Access and the type of Access for each domain User in his/her department.

5.3.2 Human Resources will instruct the IT department and its staff regarding the location of the User - whether located in the branch or Head Office - or if the User is authorized to use all network resources from all branches.

5.3.3 The IT department can and will revoke all levels of security if the User is in violation of the policies which are vital to the security of the Company's Network infrastructure.

5.3.4 No employee shall have greater information access than is necessary to capably perform his/her job function. HR personnel may have Access to confidential information and personal data in the IT Facilities and Resources relevant to HR function on a need-to-know basis for the performance of their roles and responsibilities. Employees who are given Access to portals to view (and/or update as applicable) their personal data may do so under the terms and conditions pertaining to those portals.

5.3.5 The Access of confidential information or personal data shall be recorded in the audit trail of the relevant IT Facilities and Resources.

5.3.6 All database activities, such as any changes to the database and data access activities to track unauthorized activities or anomalies, shall be logged.

5.3.7 The Access control policy is based on the following principles where reasonable:

Segregation of duties	Where practical, segregation of duties is to be implemented, so that no individual acting alone can compromise the system. This is to reduce the risk of negligent or deliberate system misuse by employees, contractors or third-party users.
Least privilege	Access must only be granted on the basis of the lowest possible level of Access required to perform the function. This limits the damage that can result from accident, error or unauthorised use of the respective systems.
Need-to-know access	Access is to be granted to Users only on a need-to-know-basis that is relevant to the job function. This also applies to third parties who provide services to the Company. A User who needs to Access information of another department must seek the approval of his/her Head of Department and the approval of the other Head of Department whose department's information is being sought by that User. The audit trail must provide information on who is accessing the information, when and what specifically was accessed to ensure accountability and easier identification, should an account be compromised. When procuring IT Facilities and Resources from third-parties or when working with partners involving IT Facilities and Resources, a formal contract must be put in place, containing or referring to appropriate information security requirements to ensure such third-parties' or partners' compliance to the Company's information security policies and standards. In granting third-party Access to the IT Facilities and Resources, appropriate security controls must be implemented according to the assessed degree of risk.

5.4 To avoid data theft or data loss, the IT department may, depending on its risk assessment and on a risk-based approach basis, install an encryption software in the hard disk of notebook computers, workstations and mobile devices provided by the Company for use by the Users.

6. PHYSICAL SECURITY

6.1 Entry into Premises

6.1.1 **Description/Rationale:** Employees, associates, contractors and visitors entering and moving about the Company's premises should have controlled and restricted access through some form of identification and authentication.

6.1.2 **Risk/Exposure:** If there is no proper identification and authentication of personnel entering and moving about the Company's premises, the Company runs the risk of people making unauthorised access to physical offices and work areas where confidential information or personal data is processed and stored to view, duplicate or steal the information. If the confidential information or personal data collected and used for identification and authentication is not properly protected, there is risk of identity theft and compromise of the security and Access control system.

6.1.3 **Preventive Measure/Action:** The Company shall implement:

6.1.3.1 Secure Access to offices and facilities using employee access cards. As an additional layer of security, the employee may be required to key in access code or to use biometrics. Employee ID card is to be displayed at all times.

6.1.3.2 Third parties and visitors are to wear their ID cards at all times. Photo images and other security data used for identifying and authenticating individuals must be securely protected.

6.2 Physical Access Control to the Server Room, Communications Equipment Room and CCTV Room

6.2.1 Only IT department personnel and staff authorized by the IT department are authorized to access the server room, communications equipment room and CCTV room.

6.2.2 All access keys, passwords, etc. for entry to the server room, communications equipment room and CCTV room or any of the IT Facilities and Resources shall be physically secured by the IT department.

6.2.3 All visitors to the server room, communications equipment room and CCTV room shall always be accompanied by IT department personnel and monitored by IT department personnel.

6.2.4 Where the Company does not have an IT department, a staff or function shall be authorised by the Company to perform the duties set out in this paragraph 6.2.

6.3 Other Areas with Physical Security Concerns

The following areas with physical security concerns shall be taken care of or are in control of other departments of the Company such as HR, administration, and security:

6.3.1 Reception Areas

6.3.1.1 **Description/Rationale:** The reception area is where visitors sign in and sign out, suppliers/vendors report to deliver goods, and couriers deliver documents and parcels/packages. It is the first stage of screening of outsiders before they are allowed access to the office.

6.3.1.2 **Risk/Exposure:** Confidential information or personal data of visitors and outsiders, if recorded in the visitor's book, could be exposed to accidental viewing by outsiders as they fill in their personal particulars. The confidential information or personal data in the visitor's book could also be browsed or photographed by outsiders without permission when the receptionists are busy or when they are not around.

6.3.1.3 **Preventive Measure/Action:**

6.3.1.3.1 To minimise exposure of confidential information or personal data contained in the visitor's book, the receptionists could record the visitor's particulars on their behalf. Instead of a visitor's book, the receptionists could request each visitor to fill in his/her personal particulars on a single sheet of paper or form. If an electronic means of registration is used (e.g., on an iPad), there must be a new blank screen for each visitor.

6.3.1.3.2 The Company could also consider an alternative to the above measures, e.g., by limiting the amount of confidential information or personal data the visitors are expected to fill in the visitor's book (e.g., name and address only, or name and mobile phone number only) or by using QR code access control system.

6.3.1.3.3 The HR or admin department shall retain hardcopies of such records in accordance with the records retention policy and all other applicable policies. Soft copies of such records shall be retained by the IT department in accordance with the records retention policy and all other applicable policies.

6.3.2 Access and Usage of Keys

6.3.2.1 **Description/Rationale:** Keys can open doors, lockers, cabinets, offices, and rooms where the Company's confidential information or personal data is kept. Procedures for controlling the movement and usage of keys are thus important.

6.3.2.2 **Risk/Exposure:** Keys in the hands of unauthorised persons could enable them to enter restricted areas to view, duplicate or steal confidential information or personal data or perform malicious acts on information assets and computer systems. Improper control over the movement of keys could lead to lost keys or unauthorised duplication of keys.

6.3.2.3 **Preventive Measure/Action:**

6.3.2.3.1 Usage of keys is to be handled with care as negligence or carelessness could lead to unnecessary exposures of confidential data and/or personal data.

6.3.2.3.2 Access to keys must only be granted to authorised persons and the relevant movement of keys and contact details must be recorded. There must be a secure keypress which can be locked at all times and the main key held by an authorised person.

6.3.2.3.3 Leaving keys within the locks is prohibited and all cabinets and rooms containing documents with personal data and/or confidential data must be locked when unattended or after office hours.

6.3.3 Video Surveillance Devices / CCTVs

6.3.3.1 **Description/Rationale:** All main entrances and exits to the Company's office premises, restricted/secure areas and other critical locations (e.g., server room and document storage areas) must be monitored to detect any intrusion or forced entry by unauthorized personnel.

6.3.3.2 **Risk/Exposure:** Main areas of risk/exposure include theft of information assets, insider sabotage, potential invasion of privacy, unauthorized disclosure of video footage and industrial espionage.

6.3.3.3 **Preventive Measure/Action:**
The department in charge of this area must assess if it is necessary to adopt the following measures on a risk-based approach:

6.3.3.3.1 CCTVs are to be positioned at strategic locations to monitor entrance/exit points where confidential information or personal data or inventory is kept/stored in addition to monitoring general premises. Notices are to be displayed prominently to inform visitors that the office or factory or warehouse premises are under CCTV surveillance.

6.3.3.3.2 The monitoring is to be monitored by trained personnel. Video footages shall be recorded and stored for at least one month (or depending on the capacity of the recording media). There must be controlled access to captured video footages as they may contain confidential information or personal data.

7. DATABASE SECURITY

7.1 **Description/Rationale:** Databases are used to store and manage data. Some could contain confidential information or personal data, and the Company needs to put in place adequate protection for these databases. Databases are often backed-up. These backups need to be similarly or even better protected than the database itself, in particular when the back-up is stored offsite.

7.2 **Risk/Exposure:** In determining where to site databases, databases must be placed in the most secure network zone and segregated from the Internet, or even the Company's internal computer Network. Like other servers and parts of the computer Network, security for databases must be regularly reviewed and improved upon.

7.3 **Preventive Measure/Action:**

7.3.1 Only authorized IT department personnel have direct Access to the database located on-site or off-site which is under the control, operation and/or oversight of the IT department.

7.3.2 The Company shall adopt a backup system as the IT department considers appropriate, taking into consideration the size of the Company, its resources and its risk assessment. Such backup system shall include as a minimum, generation backup from Monday to Friday, and may, in addition, include any of the following:

- Backup weekly or monthly to a server located on-site and off-site;
- Incremental backup nightly or at such interval the IT department considers appropriate and transfer the backup off-site;

If a third-party server is in use, the IT department shall ensure that the third-party server comply with the minimum generation backup from Monday to Friday and has an adequate backup system in place.

8. SHARED DRIVES AND FOLDERS

8.1 **Description/Rationale:** Shared drives and folders offer a convenient platform for different Users to have common Access to confidential information or personal data in electronic form from their workstations, notebook/laptop computers or mobile devices. These shared drives and folders could be sited within the third-party organisations or hosted in the cloud through external cloud service providers (e.g., Dropbox, Google Drive and iCloud). There must be proper control mechanisms to protect the confidential information or personal data and to restrict Access to authorised persons only.

8.2 **Risk/Exposure:** Shared drives and folders could be easily hacked into and the confidential information or personal data stolen or compromised if there is inadequate protection and control mechanisms. Other consequences could include the introduction of malicious code or viruses, account/service hijacking and identify theft.

8.3 **Preventive Measure/Action:**

8.3.1 Where the IT department authorizes the use of cloud-based shared services such as Dropbox, Google Drive, iCloud, a separate password to access the file must be separately sent to the recipient or a separate invitation must be sent to the recipient, as applicable. Invitation to grant third-party access must be disabled. Confidential information or personal data must not be sent over cloud-based shared services.

8.3.2 When using local shared folders within departments, the shared folders must be password-protected at a minimum (even if it is a shared password). In addition, the shared files within the shared folders that contain more sensitive confidential information or personal data must be individually password-protected, and where practical, be encrypted.

9. COMPUTER NETWORK SECURITY

9.1 **Description/Rationale:** Computer Networks allow communication between computers and devices that are connected to them. Internal computer Networks may be connected to external networks, such as the Internet.

9.2 **Risk/Exposure:** Vulnerabilities in the Network may allow cyber intrusion, which may lead to theft or unauthorised use of electronic confidential information and personal data. Wireless Local Area Networks (“WLANs”) also commonly referred to as Wi-Fi Networks, which link two or more devices wirelessly in a limited area, are common in many organisations. However, wireless Networks are generally regarded as more vulnerable because a cyber-attacker does not need to be physically connected to the Network. Traffic from wireless Networks may also be more easily intercepted through the airwaves.

9.3 **Preventive Measure/Action:**

9.3.1 Equip the Network with defence devices or software. As a minimum, the IT department shall set up a firewall.

9.3.2 Other defences that may be used to improve the security of the Company’s Network if assessed as necessary by the IT department include:

- Intrusion prevention systems (“IPS”) – a device or software application that monitors Network or system activities and prevents malicious activities or policy violations;

- Intrusion detection systems (“IDS”) – a Network security appliance that monitors Network and system activities for malicious activities and may raise alerts upon detecting unusual activities;

- Security devices that prevent the unauthorised transfer of data out from a computer or the Network, i.e., VPN;

- Web proxies, anti-virus, and anti-spyware software.

9.3.3 Review configuration settings regularly to ensure they correspond to current requirements. Design and implement the internal Network with multi-tier or Network zones, segregating the internal Network according to function, physical location, Access type, etc.

9.3.4 Apply secure connection technologies or protocols (e.g., VPN) when transmitting electronic confidential information or personal data over the Network.

9.3.5 Disable unused Internet ports that are not defined as safe by the IT department.

9.3.6 Monitor LAN/Wi-Fi regularly and remove unauthorised clients and Wi-Fi Access points.

9.3.7 Use firewalls to restrict employee access to known malicious websites.

9.3.8 Disallow third parties from conducting remote Network administration unless authorised by the IT department.

10. SAFEGUARDS AGAINST CYBER SECURITY THREATS

10.1 Public Areas with Wi-Fi

10.1.1 **Description/Rationale:** The Company’s employees may need to connect to public Wi-Fi Networks using mobile devices while on the move or outside the Company's premises. The confidential information and/or personal data stored in their mobile devices could be compromised when connecting to such Networks, especially when using unprotected Wi-Fi Networks.

10.1.2 **Risk/Exposure:** Main areas of risk/exposure include malware downloaded to the mobile devices without the Users' knowledge. The mobile devices may also be subject to virus attacks or hacking. The User could also be susceptible to identity theft.

10.1.3 **Preventive Measure/Action:** To minimise risks from public Wi-Fi Networks, it is best to avoid connecting to unsecured Networks (i.e., those that do not require passwords to connect). As a minimum, where access from public Networks is required, E-mails and open applications must use safe protocols to allow Access from public Networks. The IT department shall install an endpoint anti-virus program. The IT department may need to consider the implementation of Two-Factor Authentication and/or VPN for remote access of E-mails from public Wi-Fi Networks, depending on the risk assessment of the IT department. As an alternative to such Two-Factor Authentication and/or VPN for remote access of E-mails from public Wi-Fi Networks, either of these methods may be used: the IT Department may deploy a small Wi-Fi router (e.g., Dongle) for the employee to remote access E-mails or the employee may use his/her mobile hotspot on his/her personal mobile phone to access E-mails from public Wi-Fi Networks.

10.2 Safeguard Against Phishing

10.2.1 **Description/Rationale:** There are bogus websites and E-mails that masquerade as originating from bona fide organizations to trick the unsuspecting User into revealing confidential information or personal data such as national registration or social security or identity card number, credit card details or passwords. All staff must guard against phishing.

10.2.2 **Risk/Exposure:** If a staff is not vigilant, he/she may inadvertently give away confidential information or personal data on phishing websites or click on URL links or file attachments in E-mails that contain malware. Worse, the User could be susceptible to identity theft or he/she be held ransom by ransomware that encrypts his/her data and render it unreadable.

10.2.3 **Preventive Measure/Action:** All staff must be vigilant and be on the lookout for websites and E-mails that look suspicious. Some precautions to take are:

10.2.3.1 Do not click on the URL link or file attachment in E-mails where the content looks dubious.

10.2.3.2 Check the actual source of the email or website posting by hovering your mouse over the sender's email address or the websites URL or the embedded URL. You may discover that the source is not what you expect it to be. This mouse check, however, cannot be done on a mobile device.

10.2.3.3 Be careful when using unsecured websites asking for confidential information or personal data. Avoid websites whose URLs do not have the https prefix or the symbol of a lock.

10.2.3.4 Watch out for impersonal messages (e.g., Hello without addressing you by name) in the email purportedly from official government or purportedly from Company sources dealing with a personal matter. Other giveaways include lots of grammatical errors in the messages.

10.3 Safeguard Against Social Engineering

10.3.1 **Description/Rationale:** People with malicious intent use social, non-technical means to trick the unsuspecting individual to part with his/her confidential information or personal data. All staff must guard against Social Engineering.

10.3.2 **Risk/Exposure:** If a staff is not vigilant, he/she may inadvertently give away confidential information or personal data to people with malicious intent via the telephone, other communications media or even in face-to-face interactions.

10.3.3 **Preventive Measure/Action:** All staff must be vigilant and not fall victim to so-called social engineers. Some precautions to take are:

10.3.3.1 Always verify and authenticate the identity of the person who is asking you to disclose confidential information or personal data. You must do this even for someone who claims that he/she has been referred to you by a friend or colleague. You are to verify with your friend or colleague to ensure this is indeed the case.

10.3.3.2 Always ask the requester for the purpose of wanting Access to the information.

10.3.3.3 Always ask the requester to write in to the Company officially.

10.4 Safeguard Against Website Attacks and Web Applications

10.4.1 **Description/Rationale:** People with malicious intent can modify online websites to steal confidential information or personal data from unsuspecting users by tricking them into believing that they are providing information to access the websites services. All staff must guard against this. Two common techniques used by the malicious attacker are SQL injection and cross-site scripting. The attacker carries out the malicious act by injecting software codes or scripts into the websites input screens (where the user inputs the User ID and Password) or online forms (where the user inputs certain confidential information or personal data) and redirecting the stolen data to their own databases.

10.4.2 Websites and web applications are often used to communicate or provide services to customers or the public. A website is generally used to disseminate information whereas a web application tends to be more interactive and may allow a user to perform transactions such as buying items or checking personal account information. Websites and web applications may be connected to a database at the backend. The database may contain confidential information and/or personal data, such as information about an organization's customers.

10.4.3 **Risk/Exposure:** If a staff is not vigilant, he/she may inadvertently be tricked into giving away his/her log-in credentials or personal data, resulting in identity theft. Worse, the injected software code could insert inappropriate data into the Company's database, delete data from the database or shut a database down.

10.4.4 **Preventive Measure/Action:** It is important that the Company carries out regular vulnerability assessments and penetration tests of its websites and online applications. The IT Department is to ensure that databases are properly configured and that the database codes on the websites are written with tighter controls to minimise the risks from website attacks. If the public-facing website is hosted by a third-party, the IT department shall ensure that the third-party carry out such assessments and tests by asking for appropriate certifications and/or audit reports.

10.4.5 Where the Company hosts its own public-facing websites, precautions are to be taken against common forms of malicious activities on websites and web applications, which include, but are not limited to the following types of malicious activities:

- Injection attacks – where data is input into a web application to facilitate the execution of malicious data in an unexpected manner. The most common type of injection attack is SQL injection. This sends malicious database instructions disguised as User input from a website or web application to a database. It potentially allows attackers to access, modify and delete data.

- Cross-site scripting ("XSS") - where attackers introduce malicious programs into web pages viewed by other Users. XSS attacks can cause a website or web application to be deceived into activating malicious programs. It allows attackers to deface websites, redirect users to malicious websites, or hijack users' activities.

- Buffer overflow attacks – where malicious programs are used to send more data to a buffer, a temporary data storage area, than it was intended to hold. As buffers can contain only a limited amount of data, the extra information will overflow into adjacent buffers, corrupting or overwriting the data held in them.

10.4.6 As a minimum, the IT department will ensure that anti-virus software is installed on each workstation and strictly apply firewall rules. The IT department shall educate the Users regularly on cybersecurity and the latest updates on cyber-attacks.

10.5 Patching

10.5.1 **Description/Rationale:** Software may contain errors or bugs. Some of these lead to security vulnerabilities. Software developers generally release security patches over time to address the vulnerabilities.

10.5.2 **Risk/Exposure:** Software that is not (or no longer) supported by its developer may be at greater risk as there is no party responsible for resolving security issues. Vulnerabilities discovered are often published, hence cyber attackers are well aware of vulnerabilities available for exploiting. It is therefore important for organisations to keep their software updated or patched regularly to minimise their vulnerabilities.

10.5.3 **Preventive Measure/Action:**

10.5.3.1 The IT department shall test and apply updates and security patches as soon as they are available to relevant components of the organisation's ICT systems. These components include those described in this Policy, i.e., network devices, servers, database products, operating systems and Software Applications on computers and mobile devices, software libraries, programming frameworks, firmware (to control hardware). The IT department will review and test any updates and security patches for compatibility and other issues before these can be applied.

10.5.3.2 The IT department shall ensure that software patches are downloaded from a legitimate source and preferably, digitally signed by the software vendor, to ensure the integrity of the software patch.

10.6 Use of Social Media

10.6.1 **Description/Rationale:** The use of social media platforms such as Facebook enables the Company to do mass promotion or marketing of its products and services. It can also serve as an alternative channel for members to share with their friends or the general Facebook user population what they like or dislike about the Company's products and services. So, it is like a double-edged sword that may enhance or harm the brand reputation of the Company.

10.6.2 Social media is computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities. By design, social media is internet-based and gives users quick electronic communication of content. Content includes personal information, documents, videos, and photos. Users engage with social media via computer, tablet or smartphone via web-based software or web application, often utilizing it for messaging (Extracted from https://www.investopedia.com/terms/s/social-media.asp , accessed on 21 October 2020). Social media include social networks (e.g., Facebook, Twitter and LinkedIn) and media sharing sites (e.g., Instagram, YouTube and Snapchat).

10.6.3 **Risk/Exposure:** On social media platforms, Users tend to be more casual in their conversations and more open in sharing confidential information or personal data. Staff, thinking that they are acting in their personal capacity, may inadvertently disclose confidential information or personal data which they are not supposed to, without realising the consequences. With powerful search engines and Big Data analytics tools it is easy to trace the individual staff's association or relationship with the Company.

10.6.4 **Preventive Measure/Action:** A Social Media Policy spelling out rules on what information can or cannot be posted on social media is to be implemented so that all staff are aware of their boundaries in sharing information on social media platforms. Confidential information, personal data, defamatory statements or unlawful or illegal materials, false or misleading statements, sensitive topics, must not be shared on social media platforms in any form. Usage that is considered derogatory, discriminatory, bullying, threatening, offensive, intimidating, harassing or against the Company's code of conduct or policy is prohibited on social media.

10.7 Cloud Computing

10.7.1 **Description/Rationale:** Cloud computing is an on-demand service model for IT provisioning that is often based on virtualization and distributed computing technologies.

10.7.2 **Risk/Exposure:** It is generally regarded that organisations have the least controls with public clouds. Organisations that adopt cloud services for the management of confidential information or personal data need to be aware of the security and compliance challenges that are unique to cloud services.

10.7.3 **Preventive Measure/Action:** Where cloud service providers are unable to customise a service for the organisation, the Company must decide if the security measures put in place by cloud service providers provide reasonable security for the confidential information or personal data. Many cloud service providers publish a list of security measures offered. This can be used to help the Company make a decision on whether the level of protection is sufficient for the confidential information or personal data being stored in the cloud. The Company may refer to existing standards such as the Multi-Tier Cloud Security (MTCS) or ISO 270189, ISO/IEC 27018 for additional guidance.

10.8 Business Email Compromise

10.8.1 The Company shall have in place a two-step approval process to approve payments from the Company to payees including but not limited to reimbursements to employees, suppliers and third parties.

10.8.2 Human Firewall – Policies & Procedures

A human firewall is essentially a commitment of a group of employees to follow best practices to prevent as well as report any data breaches or suspicious activity. The importance of this added human layer of protection lies in the fact that many breaches are due to employee error. Successful hacks are caused by carelessness or simple mistakes. Software, too, makes mistakes, sometimes allowing phishing messages through or red-flagging real communications. All employees are stay vigilant in order to detect potential hazards software misses and to prevent errors from being made. Employees will be trained from time to time on such potential hazards, and will be given tips on how to counter such hazards. Such tips include, but are not limited to:

10.8.2.1 Making manual payments to a new supplier or to new bank details and:

10.8.2.1.1 Independent Call Verification of bank details is required;

10.8.2.1.2 Initiate Direct contact with supplier. Try to avoid mobile numbers; and

10.8.2.1.3 Keeping phone number on file with the Company, in supplier master or central switchboard.

10.8.2.2 Do NOT rely on email for confirming bank details.

10.8.2.3 Do NOT use a phone number from an email.

10.8.2.4 All details confirmed (account name & number, swift/sort code, IBAN, ABA, etc.).

10.8.2.5 Document the date, time, number called, where number was obtained from, person who called & person who confirmed.

10.8.2.6 Requestor attests that payment instructions have been independently verified.

10.8.2.7 Approver attests they checked that the instructions have been independently verified.

10.8.2.8 Verify if your Apps (Mobile or Web) has a two factor Authentication.

11. USER RESPONSIBILITY

11.1 In using or accessing the IT Facilities and Resources, Users must comply with the following guidelines:

System Access Requirements. Access privilege through a User Account shall be extended to all Users. A User shall be given a unique login name and password to gain access to the IT Facilities and Resources.

User ID/Name. The IT department shall issue a standardized naming convention and format of usernames.

Responsibility for Passwords. Users shall be responsible in safeguarding their passwords for IT Facilities and Resources. Individual passwords shall not be printed, stored online, or given to others. Users shall be responsible for all transactions made using their passwords. No User shall access the computer system by using another User's password or account.

Preventative Measure/Action: User IDs and passwords are to be appropriately used and protected. Each User is personally responsible for the usage of his/her own IDs and passwords which must not be shared with other individuals.

11.1.1 The following are guidelines relating to passwords:

- System passwords are to be independently assigned and used (not shared).
- Do not use the same password for a number of applications.
- Blank-field passwords (passwords without any characters) are not allowed.
- Passwords must contain the number of characters advised by the IT department from time to time.
- A combination of upper and lowercase letters, numbers and at least one special character (e.g., %, &, *) must be used in composing the password.
- Passwords must be changed at least once every quarter.
- Inactive accounts of terminated or departed employees who handled confidential information or sensitive personal data must be disabled immediately and completely. All other inactive accounts of terminated or departed employees must be disabled immediately and completely upon advice by the HR or admin department.

- Password must not be associated with anything that may be broadly familiar to the individual or others at the Company (nicknames, birthdates, etc.).
- We must not use words found in the dictionary.
- Change default passwords to strong passwords at the earliest possible opportunity.
- Users must change system-generated password upon first login.
- The same password is not allowed to be reused within the last 3 changes.
- No sharing of User Account.

11.1.2 All passwords must never be stored (or recorded) in any location that is within plain view of a casual observer (both virtually/physically).

11.1.3 Use of two-factor authentication where a password is deployed with a second layer of security, which is to be determined by the IT department according to their local requirements (e.g., use of password together with a security token or security code generated in real-time and sent via SMS or E-mail, or active directory user authentication and application-level authentication). Such two-factor authentication shall be deployed where the Company permits the Users to access the Company E-mails through webmail or through the User's personally owned mobile phone. The Users are not allowed to remotely access shared folders stored in the IT Facilities and Resources through the User's home equipment or devices personally owned by the User) Where the Company-issued equipment has broken down when the User is working from home, the User shall seek the IT department's approval before using his/her home equipment or personally-owned device and shall put in place such measures as advised by the IT department when it gives such approval.

11.1.4 Implement account lockout when the maximum number of attempts is reached, to prevent dictionary or brute-force attacks, which refer to methods of systematically checking all possible keys or passwords until the correct one is found.

11.1.5 When releasing confidential information or personal data to external parties, due diligence must be done to authenticate the requester first prior to the release of confidential information or personal data and whether the requester has the authority to access or receive the respective information. If the request is made on behalf of a third party, then an authorization letter must be produced by the individual concerned.

11.1.6 Users are required to change their passwords regularly. The frequency is to be based on the risk of damage to the individual if the data is compromised.

Exception: Department heads and head of the IT department may approve the use of the IT Facilities and Resources beyond the scope of the access policy under the following conditions:

- the intended use of IT Facilities and Resources serves a legitimate business and office interest; or
- the intended use of IT Facilities and Resources is for the individual's educational purposes and development;
  and
- the use and time of Access will be logged by the IT department including the username used for such purpose; and
- the User shall be held accountable for damages that may arise due to the improper use of the password as provided herein.

11.2 User Limitations

Using Other Users' Computers to Access Their Files A User shall not use another User's computer to Access, alter or copy a file belonging to that other User without first obtaining permission from the owner of the file. Ability to read a file belonging to another User does not imply permission to alter or copy such particular file. Users shall not use the computer system to "snoop" or pry into the affairs of other Users by reviewing the files and email of the other Users.

Using User's Own Computer to Access Other Users' Computers and Networks. A User's ability to connect to other computer systems through the Network or a modem shall not imply a right to connect to or use other systems unless specifically authorized by the business owners of those systems or those other Users.

Use of Other Public Information Services. Each Authorized User is responsible to ensure that the use of outside IT resources and networks, such as the Internet, shall in no way compromise the security of IT Facilities and Resources. This duty includes taking reasonable precautions, as provided but not limited to those stated in this Policy, to prevent intruders from accessing the Company's network without proper authorization and to prevent the introduction and spread of viruses.

Use of IT Facilities and Resources for Official Business. Users are to use IT Facilities and Resources for Official Business of the Company only.

11.3 Monitoring and Reporting Guidelines

Ownership and Right to Monitor. All IT Facilities and Resources are owned by the Company. For this purpose, the Company reserves the right to monitor and/or log all network-based activities. The User shall be responsible for surrendering all passwords, files, and/or other required resources if requested to do so, by proper authorities in the presence of his/her office head, or persons authorized by the Company.

The Company reserves the right to hold the Users liable for damages caused by the User's failure to protect the confidentiality of his or her password in accordance with these guidelines.

Reporting of Troubles or Problems. Users shall report to the IT department suspected abuse, damage to, or problems with their files. Failure to cooperate may result in the cancellation of access privileges, or other disciplinary actions. Users shall fully cooperate with the IT department in any investigation of system abuse.

Contact Person or Unit. Exception and trouble reports shall be made or relayed to the IT department so that appropriate action can be taken to address the problem.

IT Department to Deploy Monitoring Tools to Detect Improper Use. The IT department may deploy monitoring tools to detect any improper use as it deems fit and for the avoidance of doubt, the Company may exercise its right to monitor Personal Files stored in the IT Facilities and Resources in the course of such monitoring.

11.4 User Responsibility for their Laptops and Mobile Devices

The Users are responsible for taking care of their laptops and mobile devices issued by the Company and to ensure that they do not leave them in an unsafe place (e.g., exposed in the car, on the table at the mall or any unsupervised area). The Company reserves the right to deduct the replacement cost of a replacement device from such User's salary if the laptop or mobile device had been stolen or lost due to his/her negligence or carelessness.

Further the Company reserves the right to deduct the costs for the repair of the User's laptop or mobile devices if such repair is necessitated by any damage to such equipment caused by the User's negligence or carelessness.

11.5 Labelling of Confidential Information and Personal Data

11.5.1 A file, whether in electronic form or hard copy form or in any other medium, which is intended to be confidential or the nature of it may be confidential from the viewpoint of personal information, trade secrets, technical confidential information, etc., shall be marked or labelled with the word "Top Secret" or "Confidential" or "Strictly Confidential" or its equivalent.

11.5.2 **Countermeasures in case of leakage of confidential information or personal data.** Upon noticing the occurrence or the potential occurrence of any leakage of confidential information or personal data, the concerned officer or employee shall address it properly in accordance with paragraph 20.

12. VIRUS & MALWARE PREVENTION

12.1 General Guidelines

The IT department has provided and will continue to provide security solutions for virus, malware, and other malicious code. However, there are no 100% guaranteed security solutions. Each User shall take reasonable precautions to ensure that he or she does not introduce viruses into IT Facilities and Resources. All materials received on optical media or external storage or other magnetic or optical medium and all materials downloaded from the Internet or from computers or networks that do not belong to the Company MUST be scanned for viruses before being placed into the computer system.

12.2 Authorized Anti-Virus Program

No anti-virus programs are allowed to be installed in any IT Facilities and Resources, whether standalone or networked, except those prescribed by the IT department.

Installation. Users may install these anti-virus programs subject to instructions, which shall be made available by the IT department. The installation can be made through the Network. If the computer is standalone, the User shall consult the IT department.

Announcements and Updates. The IT department shall be responsible for the daily updating of the anti-virus program located in the servers. The IT department shall periodically give advisories to all Users to keep them informed of the best practices to combat viruses.

12.3 User Responsibility in Anti-Virus Protection.

The User shall be responsible for informing the IT department of any virus-infected computer.

Accessing the Internet. To ensure security and avoid the spread of viruses, Authorized Users shall not access sites that may harm the security and integrity of the IT Facilities and Resources. Examples of such sites are sites containing porn content and Warez (this is an illegal website offering free illegal software for downloading), gaming sites.

13. INTERNET USE POLICY

The Internet can be a valuable source of information and research. Thus, certain or all Users (as applicable) or offices may be provided with access to the Internet to assist them in the performance of their jobs. Use of the Internet, however, must be tempered with good judgment in order to maximize its allocated time of usage, without creating unnecessary network traffic.

13.1 Authorized Internet Connection.

The Company management will require employees to follow the Internet usage policy set out below. This policy has become common in business. Strict rules and regulations will be applied due to the following reasons:

- **Security**
  - Employees using the Internet for personal reasons may lead to Internet sites that have viruses or track an organization's information. This could potentially cause extensive damage to an organization's information systems.
- **Productivity**
  - Employee productivity is often drastically reduced if personal websites and E-mails are accessible at work.
- **Cost**
  - Using employer Internet services for personal use can increase Network traffic, which can result in purchasing larger or unneeded servers and systems to handle the amount of information processed.

Monitoring- Internet usage will be monitored and maintained by the IT department.

Only authorized personnel are allowed to have an Internet Access or connection to their computer. This account, approved by the IT department head, is provided to the Users to facilitate the task of gathering information. Direct connection to the Internet without proper approval from the IT department is strictly prohibited and Users found violating this policy may be held responsible for any security breaches and possible virus propagation and intrusion on the Network. The use of prepaid Internet connections and such other modes without prior authority from the Company is strictly prohibited.

The following rules and regulations apply:

- Internet use, on Company time, is authorized for the conduct of Company business only. Internet use brings the possibility of breaches to the security of confidential information or personal data. Internet use also creates the possibility of contamination to the Company system via viruses or spyware. Spyware allows unauthorized people, outside the Company, potential Access to Company passwords and other confidential information and personal data.

- Removing such programs from the Company Network requires IT staff to invest time and attention that is better devoted to progress. For this reason, and to assure the use of work time appropriately for work, we ask staff members to limit Internet use to work-related matters.

- Additionally, under no circumstances may Company computers or other electronic equipment be used to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related Internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

13.2 Remote Access Privileges

The Company, through the IT department, provides remote connection to the IT Facilities and Resources to Authorized Users, subject to the following conditions:

User-maintained Equipment. When the Authorized User is on remote connection, he or she shall be responsible for the computer, modem and phone line, and all accessories that are used to connect to the IT Facilities and Resources.

User Account and Password. Authorized Users shall be provided a User Account and password to connect to the remote services. The User shall be responsible to keep this User Account and password confidential, and to keep all information regarding remote Network access confidential. Propagating remote Access details is considered a security breach and may constitute ground for administrative sanction.

14. E-MAIL AND OTHER INTER-OFFICE ELECTRONIC COMMUNICATION FACILITIES

14.1 Users' Duty of Care

Users shall endeavor to make each electronic communication truthful and accurate. Reasonable care in drafting E-mails and other electronic communications shall be observed as with any other written communication. Company E-mails are strictly for business purposes only.

14.2 Prohibited Uses

14.2.1 The following shall be considered prohibited acts:

- Sending, receiving, downloading, displaying, printing, or otherwise, disseminating material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or such other similar unlawful information;

- Disseminating or storing commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political information, or any other unauthorized material;

- Sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing on-line and intranet games, engaging in online chat groups or otherwise creating unnecessary network traffic;

- Such other acts or communications that damage the integrity, reliability, confidentiality and efficiency of the IT Facilities and Resources as well as other records and documents of the Company;

- Subscribing or registering Company E-mails to any website that is not valuable to business that can cause viruses and malwares; and

- Giving Company email addresses to unauthorized personnel.

14.2.2 The User shall adopt good practices when sending Emails to internal or external parties by ensuring that the correct Email recipients are added to the addressee list.

14.3 Transmitting Sensitive Confidential Information or Personal Data

14.3.1 Description/Rationale: Transmitting sensitive confidential information or personal data of individuals, especially those pertaining to salary details, credit card details or medical history, via email or other electronic means to recipients both locally and overseas, must be done through secure means.

14.3.2 Risk/Exposure: If such sensitive confidential information or personal data is transmitted through non-secure means there could be risks of unauthorized access or modification to the data, hijack of the data, misuse of the data, or identity theft.

14.3.3 Preventive Measure/Action:

14.3.3.1 Sensitive confidential information or personal data must not be sent in the body of an E-mail but must be set out in a separate attachment to the E-mail. Password protect or encrypt attachments containing sensitive confidential information or personal data before transmission via E-mail or other electronic means. As a minimum, documents with confidential information or personal data sent via electronic media (E-mail, thumb drive, etc.) must be password-protected. The password to access the document must not be sent in the same E-mail as the document in order to avoid compromise of security. The password must be sent via a separate email or via another medium (e.g., SMS).

14.3.3.2 The IT department must either put in place or ensure that its third-party email hosting service provider put in place a log of all E-mails received and E-mails sent through the Company's E-mail system. The IT department may put in place secured ports (SSL) to control all E-mails received and sent through the Company E-mail system, depending on the infrastructure of the IT Facilities and Resources and whether an outsourced IT service provider provides services and/or infrastructure as part of the IT Facilities and Resources, and the IT department's risk assessment.

14.4 No Privacy in Electronic Communications

14.4.1 Users must never consider electronic communications to be private or secure.

14.4.2 E-mail and other electronic communications may be stored in accordance with the Company's records retention policy.

14.4.3 The Company reserves the right to monitor and/or log all network-based activities. The User is responsible for surrendering all passwords, files, and/or other required resources if requested to do so in the presence of his/her Office Head, or persons properly authorized by the Company.

15. PROPER USE AND PROHIBITED ACTS IN UTILIZATION OF THE INFORMATION TECHNOLOGY FACILITIES AND RESOURCES

15.1 General Principles of Proper Use.

A User may access only those services and parts of the IT Facility and Resources that are related to or consistent with his or her duties and responsibilities. The IT Facility and Resources shall only be used in accordance with its authorized purpose.

15.2 Prohibited Uses and Acts.

The following are considered violations in the utilization of the IT Facilities and Resources:

15.2.1 **Use of the Company IT Facilities and Resources for Criminal Activities [as Defined Under the Revised Penal Code and Other Special Laws, including but not limited to the E-Commerce Act of 2000 and the Intellectual Property Code].**

15.2.2 **Use of Copyrighted Material Without Attribution**. These include but are not limited to copying, reproduction, dissemination, distribution, use, importation, removal, alteration, substitution, modification, storage, uploading, downloading, communication, publication or broadcasting of copyrighted material not property attributed; and infringement of intellectual property rights belonging to others through the use of telecommunications networks[, which is a criminal offense under Section 33(b) of the Electronic Commerce Act. Section 33 of **RA8792,** the **E-commerce law,** states " Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of one hundred thousand pesos (P100,000) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years."]

15.2.3 **Morally Offensive and Obscene Use.** Accessing, downloading, producing, disseminating, or displaying material that is offensive, pornographic, racially abusive, culturally insensitive, or libelous in nature. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate shall not be sent by email or other form of electronic communication (such as windows messaging, bulletin board systems, news groups, chat groups) or displayed on or stored in the Company's computers or on social media. A User who encounters or receives this kind of material shall immediately report the incident to their supervisors.

15.2.4 **Hacking, Spying or Snooping.** Accessing or attempting to gain access to IT Facilities or Resources of the Company that contain, process, or transmit confidential information or personal data as well as accessing, or attempting to access, restricted portions of the system, such as e-mail lists, confidential files, password-protected files, or files that the User has no authorization to open or browse shall be prohibited [and shall carry the penalties under Section 33 of the E-commerce Law and shall be subjected to Administrative Sanctions independent of the penalties provided under the E-commerce Law]. Further, Authorized Users shall not exceed their approved levels of access, nor shall they disclose confidential information or personal data to unauthorized persons.

15.2.5 **Plagiarism.** Prohibited acts include, but are not limited to, copying a computer file that contains another person's work and submitting it for one's own credit, or, using it as a model for one's own work, without the consent or permission of the owner or author of the work; submitting the shared file, or a modification thereof, as one's individual work, when the work is a collaborative work, or part of a larger project; and such other related acts of cheating.

15.2.6 **Uses for Personal Benefit, Business or Partisan Activities**

15.2.6.1 Commercial Use. Use of the IT Facility and Resources for commercial purposes, and product advertisement, for personal profit, unless allowed under other written office policies or with the written approval of a competent authority.

15.2.6.2 Use for any partisan activities. Use of IT Facilities and Resources for religious or political lobbying, for disseminating information or gathering support or contributions for social, political, or cause-oriented group, which are inconsistent with the activities of the Company.

15.2.7 **Acts that Damage the Integrity, Reliability, Confidentiality and Efficiency of the IT Facilities and Resources**. These include but are not limited to:

- Virus infection due to connection of the IT Facilities and Resources to any unauthorised computer unit or external network;
- Acts that attempt to crash, tie up, or deny any service on the IT Facilities and Resources, such as, but not limited to sending of repetitive requests for the same service (denial-of-service); sending bulk mail; sending mail with very large attachments such as videos and pictures and sending data packets that serve to flood the network bandwidth;
- Deletion, or modification of data or records pertaining to access to the IT Facility and Resources at the time of access, or alter system logs after such access for the purpose of concealing identity or to hide unauthorized use or such deletion or modification;
- Concealment of identity, or masquerading as other Users when accessing, sending, receiving, processing, or storing through or on the IT Facility and Resources.

15.2.8 **Unauthorized Disclosure.** Copying, modification, dissemination, or use of confidential information and/or personal data such as, but not limited to: mailing lists; employee directories of any sort; operations data; research materials, in whole or in part, without the permission of the person or body entitled to give it as well as searching, or providing copies of, or modifications to, files, programs, or passwords belonging to other Users, without the permission of the owners of the said files, programs or passwords.

15.2.9 **Distribution or Dissemination of Prohibited Materials**, as considered under this Policy include but are not limited to the following:

- Any collection of passwords, personal identification numbers (PINs), private digital certificates, credit card numbers, or other secure identification information;
- Any material that enables others to gain unauthorized access to a computer system. This may include instructions for gaining such access, computer code, or other devices;
- Any material that permits an unauthorized user, who has gained access to a system, to carry out any modification of the computer programs or data stored in the system; and

- Any material that incites or encourages others to carry out unauthorized access to or modification of a computer system.

15.2.10 **Wasteful Use of Resources.** Users may not deliberately perform acts that waste IT Facilities and Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to:

- sending mass mailings or chain letters;
- spending excessive amount of time on the Internet;
- playing online or Network games;
- engaging in online chat groups;
- printing multiple copies of documents;
- printing unnecessary documents, files, data or copies of programs;
- repeated posting of the same message to as many newsgroups or mailing lists as possible, whether or not the message is relevant to the stated topic of the newsgroups or mailing lists targeted;
- sending large unsolicited files to a single e-mail address or other electronic communications facilities;
- or otherwise creating unnecessary network traffic.

16. REPAIR OF IT FACILITIES AND RESOURCES

Unauthorized Repair of IT Facilities and Resources. Only IT department personnel or personnel allowed by the IT department (suppliers, contractors, or other similar agents) are authorized to repair, open, remove, disconnect or check the IT Facilities and Resources. Users are prohibited from opening, removing, disconnecting, or detaching any peripherals or devices, especially inside the computer, without the written approval of the head of IT department. Users who violate this policy may be held liable for any loss or damage to IT Facilities and Resources.

17. USE OF PERSONAL COMPUTERSAND SMART DEVICES AND USE OF REMOVABLE MEDIA

17.1 Use of Personal Computers and Smart Devices

Officers and employees using a personal computer and/or smart device for their business operations shall observe the following provisions:

17.1.1 Using a personal computer or smart device

17.1.1.1 In principle, the Company's information systems and electronic information shall be used only on a personal computer or smart device provided by the IT department.

17.1.1.2 In the case where a User is involved in a business requiring one or more high performance or special functions that cannot be handled by a personal computer or smart device provided by the IT department, the IT department shall be allowed to obtain a terminal specifically compatible for the business at hand at his/her own discretion, and issue it to the User. However, in such case, the person concerned shall comply with relevant provisions of the IT operating standards.

17.1.1.3 Personal computers and smart devices personally owned by employees shall not be used for business purposes.

17.1.1.4 In principle, employees are prohibited from storing confidential information and/or personal data in their smart devices. If storage of such information or data in their smart devices is required strictly for work purposes, employees must store such information or data in the cloud service linked to the smart devices and not store such information or data in the in-built storage of their smart devices.

17.1.2 Software that can be used on personal computers and smart devices

17.1.2.1 Only licensed software approved by the IT department shall be used.

17.1.2.2 If it is necessary to use any other software other than those specified in paragraph 17.1.2.1 above due to unavoidable circumstances in conducting business, the issue shall be raised with the IT department to obtain permission. For the software which the IT department has granted permission to use, a security program or the like specified by the IT department shall be applied (if any).

17.1.3 Password management of personal computers and smart devices

17.1.3.1 For the personal computer and smart device in use, a password shall be set in line with the guidelines relating to passwords specified in this Policy.

17.1.3.2 The password shall be such that it cannot be easily hacked by a third party.

17.1.4 Precautions regarding the use of personal computers and smart devices

17.1.4.1 The User of a personal computer or smart device shall not be changed without permission, and if such change is necessary, the issue shall be raised with the IT department.

17.1.4.2 A personal computer or smart device shall be handled with care to prevent theft or loss when taken outside the Company's premises. In addition, upon the occurrence of a security incident such as loss or theft of a personal computer or smart device, or information leakage, the person concerned shall comply with the provision in paragraph 20.

17.1.4.3 When using a personal computer or smart device outside the Company's premises, the person concerned shall be on the alert to prevent information projected on the screen from being viewed by a third party without permission. Also, careful attention shall be paid to prevent eavesdropping such as when speaking over the phone and during web conferencing.

17.1.4.4 When not using the personal computer or smart device, the password-protected screen saver function shall be enabled and activated.

17.1.4.5 For the personal computer or smart device in use, the security update and the like specified by the IT department shall be applied.

17.1.4.6 The personal computer and smart device provided by the IT department shall not be connected to other organization's network.

17.1.4.7 When handling confidential electronic data using the personal computer or smart device provided by the IT department, the person concerned shall comply with paragraph 11.5.

17.1.4.8 Except for those approved by the IT department, when connecting to the Internet outside the Company, use the tethering function of the smart device (including hotspot) or Wi-Fi router, instead of using public Wi-Fi.

17.2 Use of Removable Media

Officers and employees using removable media for their business operations shall observe the following provisions:

17.2.1 Use of removable media in business. In principle, the electronic information of the Company shall not be saved in a removable media, regardless of whether it is confidential or not.

17.2.2 Saving data to a removable media. When saving electronic information of the Company into a removable media, the electronic file or the removable media shall be encrypted to prevent an unauthorized person from accessing the saved electronic information. Also, storing data to a removable media shall be for temporary purposes only, and the data shall be cleared immediately after the accomplishment of that purpose.

17.2.3 Taking a removable media outside the Company premises

17.2.3.1 In principle, a removable media storing the Company's electronic information shall not be taken outside the Company's premises, regardless of whether it is confidential or not.

17.2.3.2 In case where a removable media storing the Company's electronic information needs to be taken outside the Company's premises due to unavoidable circumstances, including but not limited to the storage of information in a removable media for submission to the court or to counterparties pursuant to a court order or legal proceedings, permission shall be obtained from the IT department.

17.2.3.3 A removable media shall be handled with care to prevent theft or loss when taken outside the Company's premises.

17.2.3.4 When sending a removable media by post or via parcel delivery service, a method that would assure security shall be used.

17.2.4 Applying for exemption

17.2.4.1 If the use of personal computer or smart devices or removable media deviates from the standards set out in paragraph 17 including under any of the following situations, the Company shall apply for exemption from the applicable standards in accordance with paragraph 22:

17.2.4.1.1 If employees need to save electronic information of the Company in a removable media due to unavoidable circumstances; or

17.2.4.1.2 If employees need to use their own personal computers and/or smart devices.

17.2.5 Disposal of removable media. A removable media that is no longer necessary shall be formatted if possible, and then be physically destroyed by having it scratched with a screwdriver, etc., or be cut with scissors so that it cannot be read. Shred the item if possible.

18. USE OF OFFICE EQUIPMENT IN RELATION TO CONFIDENTIAL INFORMATION AND PERSONAL DATA

18.1 **Description/Rationale:** The multifunction photocopier, printer, scanner, and fax machine are where a lot of documents containing confidential information and/or personal data are printed, photocopied, scanned, and faxed. It is thus important to have strict control measures on the use of office equipment.

18.2 **Risk/Exposure:** Without proper control measures, unauthorized persons can access the previously saved jobs in the memory of the equipment to make printouts and copies of documents containing confidential information or personal data, and even fax or email them out. Uncollected printouts and faxes can be viewed by unauthorized persons.

18.3 Preventive Measure/Action:

18.3.1 Where feasible, multifunction equipment (e.g., photocopier with fax and scanning facility) should have password control so that only authorised users can use it. Users must be reminded to collect their printouts and faxes as soon as possible and not leave them exposed and lying around.

18.3.2 Users are also to be reminded to collect their original documents after they have scanned the documents. All unwanted printouts and faxes containing confidential information or personal data must be properly destroyed using a paper shredder or a secure disposal service.

18.3.3 When the lease of the multifunction equipment expires and is to be returned to the vendor, the built-in memory must be erased to ensure no confidential information or personal data is left behind.

18.3.4 Use a fax cover sheet for documents being faxed, stating the recipient and sender details, whether the document is confidential or sensitive and the number of pages in the document. Provide advance notice to the fax recipient, such as by asking the recipient to wait at the fax machine before sending the fax.

18.4 This policy may be administered by another department in charge as directed by the IT department.

19. CLEAN DESK POLICY

19.1 **Description/Rationale:** The workstation is the place where the internal staff perform most of their work, including handling, using, processing, and sharing confidential information or personal data either in physical or electronic form. It is important that every staff is aware of his/her responsibility in protecting the Company’s information assets.

19.2 **Risk/Exposure:** The main areas of risk/exposure include:

- Documents containing confidential information or personal data exposed and lying around on the desks,
- Drawers and cabinets storing confidential files not locked,
- Door to office not locked,
- Unwanted papers containing confidential information or personal data not properly destroyed, and
- Computer terminals displaying confidential information or personal data in full view to those who are not supposed to look at the data.

19.3 **Preventive Measure/Action:** All staff must adopt a clean-desk policy, meaning that no papers, documents, or files containing confidential information or personal data are to be left exposed or unattended even for short periods. They must comply with the following requirements:

19.3.1 Restrict physical access to workstations to only authorized personnel.

19.3.2 Staff must keep confidential information or personal data in printed form locked away in drawers or cabinets when not being used or when it will be unattended for an extended period (e.g., when away for meetings, during lunch times or overnight).

19.3.3 Keys used for Access to confidential information or personal data must not be left at an unattended desk.

19.3.4 Printouts containing confidential information or personal data must be immediately removed from the printer, photocopiers or fax machines.

19.3.5 Dispose of unwanted papers containing confidential information or personal data securely using a paper shredder or a secure disposal service.

19.3.6 Lock computers when unattended (e.g., pressing Ctrl-Alt-Del and then Enter) or pressing Windows key + L (or lower case 'l'), which can only be unlocked via a password set by the staff.

19.3.7 Keep food and drink away from workstations in order to avoid accidental spills.

19.3.8 Where applicable, the office must be locked when the staff is away in order to prevent theft of or unauthorised access to documents containing confidential information or personal data. No items such as bags, mobile devices and keys (to cabinets, drawers and rooms storing documents containing personal data) are to be left unattended.

19.3.9 Computer workstations must be shut down completely at the end of the working day.

19.3.10 Computers should be anchored with a lock to the workstation if the IT department assesses this as necessary. Notebooks must be locked away if the staff is going to be away from his/her workstation or at the end of the working day.

19.3.11 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

19.3.12 Install privacy screen filters or use other physical barriers to alleviate exposing confidential information or personal data.

19.3.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

19.4 This clean desk policy may be administered by another department in the Company or as directed by the IT department.

20. INCIDENT RESPONSE POLICY

20.1 General

It is vital that computer security incidents that threaten the security or privacy of confidential information or personal data in the IT Facilities and Resources are properly identified, contained, investigated, and remedied.

This policy establishes the process for the handling of confidential information or personal data security incidents, and responsibility and accountability for all steps in the process of addressing confidential information or personal data security incidents.

20.2 Policy

20.2.1 A Security Incident (defined in para 20.3 below) against the Company must be reported to the IT department. The IT department will determine whether immediate emergency response measures, including but not limited to appropriate containment measures and applicable emergency measures that may be published by the Nippon Sanso Holdings Corporation (NSHD) head of IT from time to time, need to be taken in relation to the Security Incident reported or found and if so, to immediately deploy such emergency measures even before forming an Incident Response Team.

20.2.2 If the IT department, in collaboration with other relevant staff, determine that the incident IS a Security Incident, an Incident Response Team shall be formed. The purpose of the Incident Response Team is to determine a course of action and the timing to appropriately address the incident. Specific timelines for addressing certain incidents are given below in this section. The head of IT department or Compliance Representative (if there is no IT department) shall chair the Incident Response Team and shall designate the membership of the Incident Response Team. Normally, membership will include relevant individuals from IT, offices with primary responsibility for the compromised data, and other relevant personnel.

The timelines for addressing the following incidents are set out below:

- Loss of laptop or mobile phones issued by the Company – To report to the Company and the police (within 24 hours) and the IT department shall determine in accordance with this paragraph whether to form an Incident Response Team to investigate the incident.
- [Other examples to be inserted]

20.2.3 The IT department, in collaboration with other relevant staff, shall also determine if a reported incident IS or IS NOT a confidential information or personal data Security Incident. All Security Incidents including those concerning confidential information or personal data Security Incidents shall be reported immediately at the minimum to NSHD Chief Financial Officer, NSHD

Head of IT Department, NSHD Executive Officer, Group Corporate Planning, Nippon Sanso Holdings Singapore Pte. Ltd. regional management and the Regional Chief Compliance Officer (RCCO) with background information, and an assessment of the impact shall be provided in due course. Security Incidents shall also be reported in accordance with paragraph 20.3 below.

20.2.4 It is the responsibility of the Incident Response Team to assess the actual or potential damage to the Company caused by the Security Incident, and to develop and execute a plan to mitigate that damage. Incident Response Team members will share information regarding the incident outside of the team only on a need-to-know basis and only after consultation with and consensus by the entire team.

20.2.5 The Incident Response Team will review, assess, and respond to the incident for which it was formed according to the following factors, in decreasing order of priority:

20.2.5.1 **Containment** - Act swiftly to contain the breach (i.e., taking immediate steps to limit any further compromise of the affected system or access to or disclosure of the personal data or confidential information).

20.2.5.2 **Safety** - If the system involved in the incident affects human life or safety, responding in an appropriate, rapid fashion is the most important priority.

20.2.5.3 **Urgent concerns -** Departments and offices may have urgent concerns about the availability or integrity of critical systems or data that must be addressed promptly. Relevant IT staff or resources shall be available for consultation in such cases.

20.2.5.4 **Assess -** Work to promptly establish the scope of the incident and to identify the extent of systems and data affected and evaluate the risks posed by the Security Incident.

20.2.5.5 **Mitigation -** After life and safety issues have been resolved, identify and implement actions to mitigate the spread and harm of the incident and its consequences. Such actions might well include requiring that affected systems be disconnected from the Network.

20.2.5.6 **Preservation of evidence** - Promptly develop a plan to identify and implement steps for the preservation of evidence, consistent with needs to restore availability. The plan might include steps to clone a hard disk, preserve log information, or capture screen information. Preservation of evidence must be addressed as quickly as possible in order to restore availability of the affected systems as soon as practicable.

20.2.5.7 **Investigation -** Investigate the causes and circumstances of the incident, identify areas of weakness and recommend actions to strengthen them and determine other future preventive actions.

20.2.6 If, in the judgment of the head of the IT department or the Compliance Representative, the incident might reasonably be expected to cause significant harm to the individuals whose data has been compromised, the head of IT department, in consultation with the Compliance Representative, and the Incident Response Team will determine whether the Company should make best efforts to notify individuals whose confidential information or personal data might have been at risk due to the incident and to notify the local regulator within the required timeline and in accordance with local laws on confidential information or personal data or privacy protection. **In making this determination, the following factors shall be considered:**

- Legal duty to notify
- How long has the data been compromised
- Whether there was human involvement compromised
- Sensitivity of compromised data
- Existence of evidence that data was compromised
- Existence of evidence that affected systems was compromised
- Additional factors recommended for consideration by members of the Incident Response Team

20.2.7 The Incident Response Team shall consider reporting to the police or other governmental agencies such as the cyber security agency if they suspect that criminal acts have been perpetrated as these bodies may also offer assistance to the Company in containing Security Incident involving a personal data breach or criminal acts.

20.2.8 The IT staff shall maintain a log of all Security Incidents, recording the date, type of incident or confidential information or personal data affected, number of individuals affected (if applicable), summary of the reason for the breach, corrective measures taken, and future corrective actions to be taken.

20.2.9 The head of the IT department shall issue a report for every Security Incident describing the incident in detail, the circumstances that led to the incident, and a plan to eliminate the risk of a future occurrence.

20.2.10 If the Company does not have an internal IT department, the duties and actions of the IT department and the head of the IT department as set out in this paragraph 20 shall be undertaken by the Compliance Representative, who may delegate duties to appropriate employee(s) in the Company, provided that the Compliance Representative shall supervise and remain in control of the handling of the incident.

20.3 For the purpose of providing guidance as to the scope of a Security Incident, a Security Incident is any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information, which includes interference with information technology operation and violation of Company policy, laws or regulations.

20.3.1 Examples of Security Incidents include:

- Computer system breach
- Unauthorized access to, or use of, systems, software, or data
- Unauthorized changes to systems, software, or data
- Loss or theft of equipment storing Company data
- Denial of service attack
- Interference with the intended use of IT resources
- Compromised user accounts

The table below sets out examples of Security Incidents and the reporting lines:

Reporting event	Examples of matters to be reported	Report destination
1. Indication of a cyberattack (external attack or internal fraud)	1) If a suspicious mail was received 2) If a business device or desktop environment exhibits suspicious behavior 3) Upon noticing the fact that important data on the server has been erased/altered	1) IT department
2.Unauthorized program / malware infection	If the presence of an unauthorized program or malware infection is confirmed or suspected in the desktop environment or an email, etc. used for business	1) IT department
3. Loss or theft of business device	1) In the event of device loss 2) In the event of device theft	1) Supervisor 2) IT department

4. Leakage of confidential information or personal data	1) Upon noticing that confidential information or personal data has leaked outside the Company whether intentional or accidental 2) Upon noticing that a third party has acquired our confidential information or personal data	1) Supervisor 2) IT department 3) Data Protection Officer (if any) or Compliance Manager 4) RCCO
5. Violations	1) Upon noticing a breach of trust or violation of rules related to the information system security 2) Upon noticing a breach of contract related to information system security 3) Upon receiving a complaint from a customer	1) Supervisor 2) IT department 3) Compliance Representative and Compliance Manager

20.3.2 A Security Incident also includes any of the following:

- Incidents involving or likely to involve personal data or confidential information.
- Incidents involving legal, financial or human resource Units.
- Incidents requiring a press release or public notification, or about which media coverage is anticipated.
- Incidents that are likely to require breach notification to those affected due to laws and regulations.
- Incidents likely to result in litigation or regulatory investigation.
- Incidents involving ransomware where paying ransom is contemplated.
- Incidents involving criminal or espionage activity likely to prompt the involvement of law enforcement.
- Incidents likely to result in the compromised integrity or loss of availability of essential IT Facilities and Resources.
- Incidents likely to result in material impact to operations.
- Incidents involving a Company board member or management member.
- Other situations involving information that is considered sensitive for a variety of reasons (e.g., political, cultural, religious).
- Potential to lead to breach notification.
- Potential to lead to public notification (e.g., press releases, website announcements).

- Potential to lead to reputational risk related to the Incident.
- Potential to lead to regulatory risk.

20.3.3 Incidents that are outside the scope of Security Incidents will be classified as Routine Incidents. Characteristics of Routine Incidents include, but are not limited to:

- Common activity that can be handled with low risk, in a cost-effective manner and that involves all of the following:
  - No Company board member or management members involved.
  - Very low to no potential to lead to breach notification.
  - Very low to no potential to lead to public notification (e.g., press releases, website announcements).
  - Very low to no reputational impact related to the Incident.
  - Very low to no regulatory risk.
  - Very low to no impact to the ability to meet contractual obligations.

Routine Incidents require adequate documentation and evidence of resolution. "Adequate" documentation means the explanation will allow for later trending and analysis.

20.4 When there is doubt as to whether an incident is a Security Incident or Routine Incident, the IT department must treat Incidents as Security Incidents until data and analysis indicate otherwise.

21. COMPLIANCE

21.1 The IT department (assisted by HR and/or the Compliance Manager as necessary) will provide training on this Policy for employees on a regular basis and for such other persons as may be decided by management.

21.2 The IT department will verify compliance to this Policy through various methods, including but not limited to, periodic walk-throughs, ad hoc monitoring, internal and external audits, and through feedback to the IT department.

21.3 The Company shall from time to time verify its compliance to this Policy by conducting internal audit or external audit as it considers appropriate. Where the Company does not have an internal audit team, it may form an ad-hoc internal audit team comprising such other functions in the Company as it considers appropriate.

21.4 Questions relating to this Policy should be addressed to the IT department, HR department or Compliance Manager (as applicable), depending on the subject matter.

21.5 If the Company does not have an IT staff or internal IT department, then staff overseeing external IT service provider(s), who provide IT services to the Company, shall perform the duties of the IT department or the head of the IT department specified in this Policy under the supervision of the Chairman, President, President Director or CEO of the Company (as the case may be), taking into account best practices, advice and guidelines provided by such external IT service provider(s).

22. EXEMPTION

22.1 Exemption by the IT department. Any exemption to this Policy must be approved by the Chairman, President, President Director or CEO of the Company and the IT department in advance.

22.2 Exemption Application to NSHD. The IT department shall determine whether there is a material deviation from this Policy (a material deviation shall also include any of the scenarios described in paragraph 17.2.4) and if so, shall initiate an application for exemption from the NSHD Group CFO and IT Security department in accordance with the following procedure:

22.2.1 The request shall be made in writing using the Application Form for Exemption.

22.2.2 Exemption Applicants. The request needs to be generated locally with the approval of the local business Chairman, President, President Director or CEO of the Company and the IT department or person in charge of IT in the absence of an IT department.

22.2.3 Risk mitigation measures. The request needs to include a description of the exemption sought, the reason for the exemption, and the mitigating controls and actions which are or will be in place to ensure that the risk of the exemption does not have adverse impact on the business.

23. NON-COMPLIANCE

An employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment, in according with the Company’s internal regulation or policy.

24. RELATED STANDARDS, POLICIES, AND PROCESSES

Data Protection Policy (when approved)
Records Retention Policy (when approved）
Use of Social Media Policy (when approved)

25. UPDATE TO THIS POLICY

The Company, through the IT department, may update the policy considerations provided herein as often as necessary. Such updates may be communicated via E-mails and consolidated in this Policy from time to time.

(Draft as of 24 May 2021 PM)