E-POLICY

This E-policy was updated with reference to the Sunway Information Security Policies, specifically section 4, End-user Security, which details acceptable usage standards for users to adhere to.

TABLE OF CONTENTS

1.0 OBJECTIVE

While Information Assets will be provided to enable Users to satisfactorily complete their duties, the purpose of this policy is to establish a guideline for the provisioning of the Information Asset by the Sunway Group and the associated responsibilities of the Users when accessing these Information Assets

2.0 SCOPE

This Policy applies to the Sunway Group and to all users of information assets owned by the Sunway Group, including users of the Sunway Group, vendors, business partners, contract personnel and functional units regardless of geographic location.

This Policy covers all Information Systems (IS) environments operated by or on behalf of the Sunway Group. IS environments including the total environment and all documentation, physical and logical controls, personnel, hardware (e.g. servers, desktop and network devices), software, and information.

You are required to read, understand and comply with this Policy and other related policies, standards, and procedures. If any clarification regarding the contents of this document is required, the following should be consulted as applicable: Systems Administrator, Security Administrator, or Group Human Resources.

All usage of Information Assets areas subject to monitoring and full access by Sunway Top Management

3.0 DEFINITIONS / ABBREVIATION

Term	Definition
Compliance	State of conformance with the mandatory controls indicated in this policy, indicated with the word “must”.
Chain email	Chain emails are those that, in the body or subject of the message, ask the recipient to forward the email on to multiple people. Many chain letter emails are hoaxes and are often considered to be a security and privacy risk
Copyright	Legal protection giving the author or owner rights over the copying, use and commercial exploitation of the materials, for example through software licenses. Copyright is a form of intellectual property.
Cryptography, cryptographic, ‘crypto’	The mathematical science behind ‘secret writing’ involving the use of mathematical algorithms to transform readable plaintext into unreadable cypher-text and vice versa.
Enterprise communications	Forms of communication enabled by Information Technology, enhanced for use in an enterprise environment. E.g. email, instant messaging (Microsoft

	Teams), message board/ social media-style collaboration tools / blogging (Microsoft Yammer), virtual meetings, video conferencing, etc.
Information asset	Includes both structured and unstructured data, (e.g. data, database, proprietary knowledge, ideas, plans, communications, documents, messages, experience, insight, etc.). Basically, valuable information content that requires protection against information security risks. May belong to the Sunway Group, or to a third party but placed under the care of the Sunway Group (e.g. personal data).
Information Processing Facility	Any system, service, infrastructure, or physical location that houses information assets, owned or leased by the Sunway Group
Intellectual Property (IP)	A collection of intangible legal rights that allow the owner of intellectual property to determine how the intellectual property is used , for example through software licensing/copyright, patent, trademark or contract law.
License	Permission granted by the owner of IP (such as software) for someone to copy and/or use them subject to certain conditions.
Mass mailing	Emails sent to a large group of people/ staffs (e.g. all Users, or to complete list of Users within department)
Malware	Malicious code or malicious software are programs that are covertly inserted into a system with the intent of damaging or destroying Sunway Group network infrastructure and services.
Network	This includes all Sunway Group network infrastructure elements and support systems, including servers, computers, and networking devices that facilitate or regulate the transmission of data. This also includes external connections to other organisations or subsidiaries.
Trojan	A program that appears legitimate, but performs illicit activities when it is run. It may be used to steal data (e.g. password information), create a system vulnerability, or simply destroy programs or data on the computer. Trojans are similar to viruses, except that it does not replicate itself.
Unlawful Material	Any material which is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate.
Users	Any users (be it employees, contractors, vendors, agents, advisors, consultants or other third party personnel), both domestic and overseas, who has been authorised by the Sunway Group to access any information processing facility or information asset belonging to the Sunway Group
Virus	Self-replicating code that creates copies of itself and distributes/ infects those copies to other files, programs or computers. Computer viruses could merely slow down a system, or could corrupt data.
Mobile Device	A portable computing device such as a smartphone or tablet computer
Operating system	The low-level software that supports a computer's basic functions, such as scheduling tasks and controlling peripherals.
Passcode	A string of characters used as a password, especially to gain access to a computer or smartphone.

Passcode Timeout	An interrupt signal generated by a program or device that has waited a certain length of time for some input but has not received it. Many programs perform time-outs so that the program does not sit idle waiting for input that may never come.
Password Complexity	A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorised access. A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or parts of the user's own name.
Encryption	The process of converting information or data into a code, especially to prevent unauthorised access.
Authentication	The process or action of verifying the identity of a user or process.
Anti-Virus	(of software) designed to detect and destroy computer viruses
Firewall	To protect (a network or system) from unauthorised access with a firewall.
Virtual Private Network	A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.
Jail Broken	To modify (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorised software.
Rooted	Gaining access to the lowest level (root level) of the Android operating system, which is prohibited on stock devices. Rooting gives the user administrator rights to alter the OS, tweak the hardware and unlock the phone from its carrier.
e-Meeting	An e-meeting is a meeting between at least two people who can see each other but are not in the same place. An e-meeting is a web-based meeting or conference format that allows people to see and hear each other. Participants talk in real time and may even make presentations with visual aids such as charts and graphs
HTTPS	Stands for Hypertext Transfer Protocol Secure (HTTPS) and is a variant of standard web transfer protocols (HTTP) which adds a layer of security to data in transit.
SSL	Stand for Secure Sockets Layer and is a secure protocol that protects information sent over the internet.
AI	Artificial Intelligence (AI) refers to the capability of a machine or computer system to perform tasks that typically require human intelligence. These tasks include learning from experience, understanding language, recognizing patterns, solving problems, and making decisions.
ChatGPT	ChatGPT is a type of artificial intelligence (AI) developed by OpenAI. It is designed to understand and generate human-like text based on the input it receives. Essentially, ChatGPT can hold conversations, answer questions, provide information, and assist with various text-based tasks by predicting the most appropriate responses using its extensive training data.

4.0 POLICY

4.1 Acceptable Use

A guideline for the acceptable use of Sunway Group information assets, information processing facilities and network infrastructure in order to minimise the risk of:

- Inadvertently accessing unsuitable materials;
- Unauthorised equipment being connected to the system;
- Potential disruption of Sunway Group operations;
- Information disclosure; and
- Users performing unauthorised activities.

4.1.1 PROHIBITED USE

Sunway Group information system and processing facilities must not be used for the creation or distribution of any disruptive or offensive messages.

Users must not post / upload information / material that could cause damage or disruption of Sunway Group operations. Users must not use the system to access material that is:

- Profane or obscene,
- Advocates illegal acts,
- Advocates violence, or
- Advocates discrimination towards other people.

4.1.2 UNAUTHORISED ACCESS / DISRUPTION OF SERVICES

Users must not attempt to gain unauthorised access to information system and processing facilities or go beyond their authorised access. This includes attempting to log in through another person's account or access another person's files. Users must not make deliberate attempts to disrupt Sunway Group systems or destroy data by spreading computer viruses, scanning the network or by any other means.

Users must not set up any unauthorised internet services (such as email, proxy, web servers etc.) within the Sunway Group without prior approval. All such services must have proper justification and must be endorsed by management before being implemented. The respective management reserves the right to reject the request, if the requested change could potentially endanger the security posture of Sunway Group network infrastructure and systems.

Any tapping on the network by the means of using network probes, network monitoring tools or software is strictly restricted. All such activities must have proper justification and must be approved by the respective management.

4.1.3 UNAUTHORISED HARDWARE, SOFTWARE AND TOOLS

The use of any software or tools generating huge traffic on the network is strictly prohibited. Use of any form of hacking and vulnerability assessment tools (be it hardware or software) is strictly prohibited, except for Compliance Reviews and Assessment or Audit purposes.

Users shall not use any software, tools and platform not authorised by Group IT for enterprise communication. Refer below for communication mediums approved by Group IT:

- Email: Microsoft Outlook
- Communication and collaboration: Microsoft Teams
- File sharing and storage: Microsoft OneDrive

4.1.4 COPYRIGHTS

Users must respect the rights of copyright owners. Copyright infringement occurs when a work that is protected by copyright is inappropriately reproduced. Where a work contains conditions regarding its use, these must be followed.

All proprietary information, including but not limited to trade secrets, copyrighted materials, and confidential business information, must be protected when using third-party AI systems e.g. ChatGPT. Users shall ensure that no proprietary information is inadvertently or intentionally disclosed to third-party AI systems without proper authorization and safeguards.

When using third-party AI systems, Users shall comply with all applicable copyright laws and regulations. Users are prohibited from using third-party AI systems to generate, reproduce, or distribute content that infringes on the copyrights of others.

User shall exercise caution when sharing data with third-party AI systems to prevent the unauthorized disclosure of sensitive or proprietary information. All data shared with third-party AI systems must be anonymized and de-identified to the extent possible to protect Sunway Group's intellectual property and privacy rights.

4.1.5 COMMUNICATION OF TRADE SECRETS

Users shall not send, transmit or otherwise disseminate any propriety data, trade secrets or other confidential information about Sunway Group of Companies. Any unauthorised dissemination of this information may, in additional to disciplinary action to be taken by the management, leading to criminal or civil legal action being taken against that individual Users.

4.1.6 USE OF SOCIAL MEDIA NETWORK

Any Users accessing and using social media network shall not:

- Post or display any Unlawful Material;
- Post or display materials that may promote discrimination on the basis of race, gender, national origin, sexual orientation, religion, disability or any unlawful material which may breach or violate any provisions of the laws;
- Post or display any photos or multimedia files depicting the premises, products or services of the Sunway Group unless such photos or multimedia files have been approved for public dissemination; and
- Write any comments that in any way disparaged the Sunway Group of Companies.

Users are reminded that the law of defamation, sedition and other laws that protects the reputation and privacy are applicable to postings on social media network and Users are urged to exercise due care when using social media network.

4.1.7 MONITORING

All communications and stored information sent, received, created or contained within Sunway Group systems are the property of the Sunway Group and must not be considered as private. Such communication and information may be accessed and monitored by personnel authorised by the Sunway Group in accordance with the company policies or governing laws and regulation.

4.1.8 DATA ROAMING

For users traveling overseas for business purposes with subscription to the corporate telecommunications plan, please turn off your home country data roaming plan and select Company telecommunications provider data roaming partner to avoid unnecessary phone charges or use secure Wi-Fi.

4.2 Enterprise Communications

A guideline for the acceptable use of Sunway Group enterprise communication systems. This E-Policy is not in any way intended to impede the communications of users.

4.2.1 ACCEPTABLE ENTERPRISE COMMUNICATIONS USE

Enterprise communications may only be used for official correspondence between users and to external parties. Sunway Group's enterprise communications services are organisational resources provided for business purposes. Any personal use must be of a very minimum level, and:

- Must not interfere with business functions
- Must not be associated with any for-profit outside business activity
- Must not have negative impact on the reputation of the Sunway Group.
- Mass mailing is prohibited unless authorised

Any organisation-related communications not limited to email, e-meeting and file sharing shall be strictly communicated through the user's account as well as software, tools and platform provided by Sunway Group. Below are the communication mediums approved by Group IT:

- Email: Microsoft Outlook
- Communication and collaboration: Microsoft Teams
- File sharing and storage: Microsoft OneDrive
- Questionnaire and Survey: Microsoft Forms

Users could refer to the guidelines provided by Group IT on the best practice of using these mediums which can be found in HR Portal:

- Guideline for Microsoft Teams - GIT/Security Guideline/COMP&GOV/D1
- Guideline for Microsoft OneDrive - GIT/Security Guideline/COMP&GOV/D2
- Guideline for Microsoft Forms – GIT/Security Guideline/COMP&GOV/D2

Users shall not send company related information through their personal communications account. These include, but are not limited to: Gmail, Yahoo, Hotmail, Facebook, Twitter, Skype, etc.

Users shall not auto forward any corporate email communication to another email account other than Sunway Group corporate email domain. Doing so is strictly prohibited and it is going against clause 4.1.5 Communication of Trade Secrets. All email communication must be made using Sunway Group corporate email domain.

Users are encouraged to do regular housekeeping by archiving and deleting emails that are no longer required. Huge files should be compressed before they are sent out. Document links should be used instead of file attachment for file or database which is required to be sent to many recipients.

Users are responsible to ensure that collecting of personal information must be adhering to Malaysia's PDPA act and regulation. Point of references can be found in the PDPA Compliance Manual or by engaging the respective BU PDP Officers.

4.2.2 OFFENSIVE CONTENT

Sunway Group enterprise communications services must not be used for the creation or distribution of any disruptive or offensive messages, which includes:

a) Offensive comments on:
   - Racial remarks
   - Sexual Orientation
   - Gender
   - Religion
   - Disability
b) Political statements
c) Pornography
d) Abusive Language/Vulgarity

Users who receive such messages should report the matter to the immediate superior at once, with the information of the Sender as well as the Timestamp of the message for investigation of misconduct.

4.2.3 CLASSIFIED CONTENT

Users of Sunway Group are strictly prohibited from sending any confidential or sensitive marked information with regards to the company to any external parties, via the enterprise communications services of the Company. These include, but not limited to the following:

- Business proposals/ plans;
- HR personal information; and
- Personal records.

In any circumstance, if the sending of classified content is required, users must use some form of security control to ensure that the communication and content is delivered to the desired recipient in a secure manner. Security controls include, but not limited to the following:

- Encryption
- Password Protection
- Mark Subject with Confidential

4.2.4 ACCESS TO OTHER'S ENTERPRISE COMMUNICATIONS ACCOUNTS

User may access another user's enterprise communications account, subject to the following conditions:

a) Owner of the account voluntarily grants access to his or her account to another User due to work-related reasons. In this scenario, the owner of the account can grant access directly to another User.
b) In the event that Users need to access another User's account for work-related purposes, but the owner of the account is not able to give authorisation due to various reasons, a formal requisition for approval with justification will need to be raised by the following personnel:
    i. Immediate Superior – Requestor
    ii. Supported by – Head of Department
    iii. Recommended by – Head of Company/PCM

c) The requisition for approval will need to be approved by the following parties:
    i. Head of Group Human Resources (GHR), and
    ii. Chief Information Officer (CIO) of Sunway Group.

d) In the event that the Purpose of accessing a User's account is for an investigation, the same process as per subsections 4.2.4(b) and (c) apply.

Upon obtaining all the relevant approvals from the respective parties as indicated in subsections 4.2.4(a), (b) and (c) above, the Users will be granted access to the account, or backup copies of the contents of the account, for a maximum of seven (7) days only. Any request for access beyond 7-days duration must be accompanied with legitimate justifications for approval.

4.3 Clear Desk and Clear Screen

This is a set of guidelines which reduce the risk of a security breach, fraud or information theft caused by documents, information and/or data being left unattended in the premises of the Sunway Group. It applies to all information that is owned, created, collected, managed, stored and disseminated (both internally and externally) by the Sunway Group, in physical and electronic formats.

4.3.1 CLEAR DESK

Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office / room doors must be locked if left unattended. At the end of each session in the meeting room, all sensitive information should be removed from the room and stored in a locked area. Confidential, sensitive or classified information, when printed, should be cleared from printers immediately.

4.3.2 CLEAR SCREEN

Computer terminals should not be left logged on when unattended and should be password protected. The Windows Security Lock should be set to activate when there is

no activity for a short pre-determined period of time. The Windows Security Lock should be password protected for reactivation. Users should log off or lock their machines when they leave their cubicle.

4.4 Password Management

4.4.1 ACCEPTABLE MANAGEMENT OF PASSWORD

Formal password management procedure must be defined by Business Units to ensure the use of strong personal passwords outlining at minimum, the following requirements:

a) Password handling
Passwords must be kept strictly confidential and must not be shared with anyone. Passwords should never be written down or stored online.

b) Password change
The users must change passwords to prevent their ID from being compromised. This is usually done during a periodic system-prompted password change, the 1st log-on attempt, or upon suspicion of any access leaks.

c) Password validity
Passwords for critical business applications (such as JDE, IFCA, etc.) must be changed periodically.

d) User account lock out policy
Preventive measures must be enforced to ensure that multiple attempts to use incorrect user's passwords will cause the account to be locked. This is to prevent unauthorised users from accessing it.

e) Password uniqueness policy
User's account with special privileges (such as system administrator accounts) should have a password that is unique, compared to all other accounts held by that user.

f) Revealing of Passwords
Password must not be revealed in any way, verbally or non-verbally.

4.4.2 PASSWORDS DO NOT IMPLY PRIVACY

The granting of passwords to gain access to the Information Asset or to encode any particular file or message does not imply that the User has an expectation of privacy in the material he/she created, received or stored on the Information Asset. The Management must have the right to access those materials at any time when the need arises.

4.4.3 CREATION AND MAINTENANCE OF PASSWORDS

Required Creation & Maintenance of Passwords:

a) Passwords should consist of a minimum of 8 characters;

b) Passwords should consist at least 2 or more types of characters from the following groups:
    i. Lower Case Letter, e.g. y, o, g etc. or Upper Case Letter, e.g. B, I, W etc.;
    ii. Numeric, e.g. 1, 5, 9 etc.;
    iii. Special characters, e.g. @, !, $ etc.
c) Passwords should be changed no longer than every 90 calendar days.
d) Passwords used should not be the same for the last 5 previously used passwords.

Samples of password: $unw4yGr0up, $uP3rM@n, P0w3r@nG3r, U1tr@M@n.

4.5 Malicious Code Protection

The Sunway Group network infrastructure is susceptible to information security threats. One of the major threats is the introduction of malicious codes into the Sunway Group network infrastructure. Malicious codes include computer virus, worms, trojans, ransomware, and other malware.

Considering the criticality of Sunway Group network infrastructure and services, comprehensive protection needs to be implemented to protect the Sunway Group network infrastructure from the malicious codes. This document demonstrates the dedication and commitment of the Management in protecting the Sunway Group network infrastructure from malicious codes.

The objectives are as follow:

a) To establish malicious code prevention measures, which must be met by all PC's connected to the Sunway Group.
b) To ensure effective virus detection and prevention in the Sunway Group network infrastructure.

4.5.1 ANTI-VIRUS SOFTWARE

The ITSSC Infrastructure Department and respective IT Heads of other Business Units must be responsible to ensure that all network infrastructure connected to Sunway Group's system are installed with an approved antivirus software by Group IT.

In addition, all areas within Sunway Group must ensure that the following exists:

a) Formal policy prohibiting the use of unauthorised software on production systems;
b) Indicate protective measures to protect against risks associated with obtaining files and software from any network medium; and
c) The anti-virus software must be scheduled to run at regular intervals.

4.5.2 LICENSES

The ITSSC Infrastructure Department and respective IT Heads of other Business Units shall be responsible to ensure that adequate numbers of licenses are available for all operating systems and software connected to Sunway Group's system.

4.5.3 VIRUS DEFINITIONS / UPDATES

The ITSSC Infrastructure Department and respective IT Heads of other Business Units must be responsible to ensure that all the anti-virus software are updated with the latest

virus definitions and scan engines, based on the recommendations of the Anti-virus Product Vendor.

4.5.4 MONITORING OF ANTI-VIRUS PROTECTION STATE

The ITSSC Infrastructure Department and respective IT Heads of other Business Units must be responsible to perform on-going monitoring to ensure that deployed anti-virus software (including definitions, patterns, engines, etc.) are up to date in accordance to anti-virus product vendor support. A formal process must be defined outlining the process to be followed in case the anti-virus protection is outdated.

4.5.5 ACCESSING THE INTERNET

When using information assets provided by the Sunway Group, users must only access the Internet through the Internet firewall installed on the Information Asset to ensure security and to avoid the spread of viruses. Accessing the Internet directly by modem (be it broadband, 3G or otherwise) is strictly prohibited.

Use of the Internet must be guided with common sense and good judgment. The User's access to the Internet will be revoked in the event Users are found to have abused the use of the Internet or violated any of the rules in this E-Policy. Users may also be subject to disciplinary action, including possible termination upon the occurrence of such an event.

4.5.6 OPERATING SYSTEM

The ITSSC Infrastructure Department and respective IT Heads of other Business Units shall be responsible to ensure that all operating system connected to Sunway Group's system are constantly updated to the latest supported version and contain the latest security patches. With justifiable reasons, those operating system not updated with the latest supported version shall be mitigated with treat protection solution.

4.5.6 PUBLIC FACING WEBSITES AND APPLICATIONS

Public facing websites and applications to the internet are required to follow these security controls:

a) Only HTTPS connections are allowed.
b) Use only supported versions of TLS secure protocols.
c) Reputable SSL certificate of authority.
d) For detail controls, refer to Group Cybersecurity Policy.

4.6 Compliance

4.6.1 IDENTIFICATION OF APPLICABLE LEGISLATION

The design, operations, management and use of Sunway Group assets must comply with all applicable legal, regulatory or contractual security requirements. The specific controls and individual responsibilities to meet these requirements must be similarly defined and documented.

4.6.2 INTELLECTUAL PROPERTY

The Sunway Group will recognise and respect intellectual property associated with its information asset. All Users must comply with:

a) Copyright restrictions associated with proprietary material, software, and designs acquired and owned by Sunway Group
b) Licensing requirements limiting the usage of products, software, designs and other material acquired by Sunway Group.

The Sunway Group must ensure compliance with product copyright restrictions and licensing requirements.

All Users are responsible to ensure only authorised software is used in the Sunway Group. Proprietary software products are usually supplied under a license agreement that limits the use of the products to specific machines and may limit copying to the creation of back-up copies only. The following controls must be applied:

a) Publish a software copyright compliance policy which defines the legal use of software and hardware products;
b) Software acquisition must comply with approved procurement processes and procedures;
c) Appropriate asset registers must be maintained to track software, so that usage does not exceed the allowable copies and installations;
d) Proof and evidence of ownership of licenses, master disks, manuals, etc. must be maintained;
e) Controls must be implemented to ensure that any maximum limit of Users permitted is not exceeded; and
f) Regular checks must be performed to ensure that only authorised and licensed software are installed.

Controls must be implemented to ensure that software are disposed or transferred to other parties appropriately and asset inventory are updated accordingly.

Any content generated using third-party AI systems that includes Sunway Group-owned information must be treated as Sunway Group property and adhere to existing policies on intellectual property. Users shall ensure that the use of third-party AI systems does not result in the unauthorized use or distribution of Sunway Group-owned copyrighted materials.

4.6.3 SAFEGUARDING OF ORGANISATIONAL RECORDS

Sunway Group organisational records relating to information security must be protected and stored in accordance with: -

a) Sunway Group policies on the maintenance of such records;
b) All applicable laws and regulations in Malaysia;

The records must be categorised into record types, each with details of retention periods and type of storage media. Any related cryptographic keys (if applicable) associated with encrypted archives or digital signatures, must be kept securely and made available to authorised personnel only when needed.

The records must be protected based on the relevance and importance of the records, and must be stored in a manner appropriate to the media on which they are recorded.

Sunway Group organisational records relating to information security include, but are not limited to, system logs, audit logs, configuration setting records, change control logs, and user access authorisation documentation in electronic or hard-copy format.

4.6.4 PREVENTION OF MISUSE OF ASSET

Sunway Group assets are provided for business use only.

Any use of Sunway Group assets for non-business or unauthorised purposes must be regarded as improper use of Sunway Group assets. If such activity is identified, the respective IT Head of the Business Unit must be notified, in order for the appropriate disciplinary action to be carried out, in accordance with Sunway Group's Code of Ethics. If the activities identified were caused by an external party, they may be referred to Group Human Resources for further investigation, in accordance with Sunway Group Policies and Procedures.

4.6.5 SYSTEM ADMINISTRATORS RIGHTS

Sunway Group's appointed Systems Administrators does not have the rights to access and view the files and databases meant for other users through the use of Administrator Password unless with prior written authorisation and approval from the respective IT Heads of other Business Units.

4.6.5 DATA SHARING

Intra-Group Data Sharing Policy found within Sunway Group's PDPA Compliance Manual intends to provide guidance on the sharing of Personal Data within and across Sunway Business Units and third party which only take place if the Data Users ensure an adequate level of protection of Personal Data it processes and that such processing is in compliance with the Act.

This Policy shall apply to all incidents of Data Sharing and shall set forth the policies and guidelines applicable to Personal Data shared within Sunway Group to ensure the effective and secure storage of Personal Data and compliance with Sunway Group's obligations under the Act in processing the Personal Data.

Where Data Sharing within Sunway Group is necessary and is in accordance with Intra-Group Data Sharing Policy, Data Sharing should be strictly limited to only authorised employees on a "need-to-know" basis only and access to such Personal Data should be reviewed periodically.

Each Data User shall ensure that all Personal Data is not disclosed to third parties unless such disclosure is permitted and in accordance with Sunway Group Personal Data Disclosure Policy. Each Data User shall maintain a register of disclosures to third parties, which shall also include disclosures of Personal Data made within Sunway Group.

For more information, please refer to Sunway Group's PDPA Compliance Manual.

4.7 Mobile device security & Control

To ensure governance over the defined practices, responsibilities and procedures for the usage of enterprise and/or personal mobile devices that Sunway Group authorised to access to its information asset.

4.7.1 SECURITY REQUIREMENT

i. Users must accept that, when accessing information asset using mobile devices, security features is being enforced on mobile devices. The security features implemented may include (but not limited to), passcode, passcode timeout, passcode complexity and encryption.
ii. All mobile devices must be secured and require authentication to unlock.
iii. All mobile devices must be configured automatically to lock immediately after a predefined period of inactivity.
iv. Sunway Group reserves the right to install, configure or remove secure communication application(s) such as (but not limited to) Anti-Virus (AV), firewall and Virtual Private Network (VPN) on the user's mobile devices as long as users are accessing Sunway Group information.
v. Users must take the responsibility to prevent others from gaining access to their mobile devices. Users must bear the responsibility for every action taken when accessing Sunway Group information via mobile devices.
vi. Users must not provide mobile access details to any other individuals.
vii. Use of mobile devices that have been subjected to any methods of changing and/or bypassing the built-in security features and controls (i.e. 'Jail Broken', 'Rooted', etc.) are strictly prohibited.
viii. Sunway Group retains the right to remove access rights, mobile applications and information asset in user's mobile device if misused according to the security requirement.

4.7.2 RESIGNATION OR TERMINATION OF EMPLOYMENT

i. Sunway Group information asset in user's mobile devices remains the property of Sunway Group even when the user leaves the company.
ii. Sunway Group reserves the right to remove Sunway Group mobile applications and information asset in user's mobile devices in the event of resignation or termination.
iii. Former users are not authorised to restore any data or applications that originate from their past relationship with Sunway Group.

5.0 RESPONSIBILITY

Management is responsible for the necessary actions in the event of policy violation. Group Human Resources is responsible to administer the E-Policy for the Sunway Group.

It is the responsibility of each Users to ensure that any use of outside computers and networks, such as the Internet, do not compromise the security of the Information Asset. These duties include taking all reasonable precautions to prevent intruders from accessing the Sunway Group network and to prevent the introduction and spread of viruses.

All Users must respect the confidentiality of electronic communications belonging to other individuals. Save for cases where explicit authorisation has been granted by the respective IT Heads of other Business Units and the owner, users must not access files, computer or other networks, alter or copy files belonging to any other Users.

Any Users who violates the E-Policy will be personally responsible and/or shall keep Sunway Group fully indemnified from any such actions.

6.0 NON-COMPLIANCE

Suspected or known violations of the E-Policy must be confidentially reported to the management of the department in which the violation occurs. Any users found to have violated this E-Policy may be subjected to disciplinary action, up to and including termination of employment.

7.0 FREQUENCY OF REVIEW

This E-Policy may be amended or revised from time to time as the need arises without having to provide any reasons. Users will be informed through the Sunway Group Intranet about all amendments and revisions.

Date	Item Amended	PIC
7 April 2011	New	IT SSC (Kevin Khoo) Group HR (Harithah Mohd Harith) Group Legal (Cindy Goh)
20 July 2015	3. Definitions Changed Computer Resources to Information Assets Changed Authorised User to Users Added new definitions / abbreviation i. Compliance ii. Chain email iii. Copyright iv. Cryptography, cryptographic, 'crypto' v. Enterprise communications vi. Information processing facility vii. Intellectual property viii. License ix. Mass mailing x. Malware xi. Network xii. Trojan xiii. Virus New clauses added 4.1 Acceptable Use 4.3 Clear Desk And Clear Screen 4.6 Compliance Enhanced clauses 4.2 Electronic Mail (E-Mail) to Enterprise Communications 4.4 Password Management 4.5 Malicious Code Protection 5.0 Frequency of Review 6.0 Responsibility	Group IT (Ivan Chew Boon Yik) IT SSC (David Low Swee Nyen) Group HR (Tang Choong Shyuan)
21/07/2017	Existing clause edited 4.2.3 CLASSIFIED CONTENT 4.4.3 CREATION AND MAINTENANCE OF PASSWORDS 4.5 MALICIOUS CODE PROTECTION	ITSSC (Eddie Hau & Michael Louis Singh) Group IT (Ivan Chew Boon Yik)
04/10/2018	Added additional clause: 4.7 Mobile Device Security & Control and its sub category	GIT (Michael Louis Singh)

	Added and amended the following: • definitions based on clause 4.7 such as I. Mobile Device II. Operating system III. Passcode IV. Passcode Timeout V. Password Complexity VI. Encryption VII. Authentication VIII. Anti-Virus IX. Firewall X. Virtual Private Network XI. Jail Broken XII. Rooted • Replaced 'employees' and 'user' to 'users' • Replaced 'the company' with 'Sunway Group'	
08/04/2020	Added and amended the following: • Changing words like recognize and organization to recognise and organisation • Forms of communication enabled by Information Technology, enhanced for use in an enterprise environment. E.g. email, instant messaging (Microsoft Teams), message board/ social media-style collaboration tools / blogging (Microsoft Yammer), virtual meetings, video conferencing, etc. • An e-meeting is a meeting between at least two people who can see each other but are not in the same place. An e-meeting is a web-based meeting or conference format that allows people to see and hear each other. Participants talk in real time and may even make presentations with visual aids such as charts and graphs • 4.1.3 UNAUTHORISED HARDWARE, SOFTWARE AND TOOLS o Users shall not use any software, tools and platform not authorised by Group IT for enterprise communication. Refer below for communication mediums approved by Group IT: ▪ Email: Microsoft Outlook ▪ Communication and collaboration: Microsoft Teams ▪ File sharing and storage: Microsoft OneDrive • 4.2.1 ACCEPTABLE ENTERPRISE COMMUNICATIONS USE o Any organisation-related communications not limited to email, e-meeting and file sharing shall be strictly communicated through the user's account as well as software, tools and platform provided by Sunway Group. Below	GIT (Michael Louis Singh)

	are the communication mediums approved by Group IT: ▪ Email: Microsoft Outlook ▪ Communication and collaboration: Microsoft Teams ▪ File storage: Microsoft OneDrive o Users could refer to the guidelines provided by Group IT on the best practice of using these mediums which can be found in HR Portal: ▪ Guideline for Microsoft Teams - GIT/Security Guideline/COMP&GOV/D1 ▪ Guideline for Microsoft OneDrive - GIT/Security Guideline/COMP&GOV/D2 • 4.5.6 OPERATING SYSTEM o The ITSSC Infrastructure Department and respective IT Heads of other Business Units shall be responsible to ensure that all operating system connected to Sunway Group's system are constantly updated to the latest supported version and contain the latest security patches. o With justifiable reasons, those operating system not updated with the latest supported version shall be mitigated with treat protection solution.	
09/08/2021	<u>Added and amended the following:</u> • 3.0 DEFINITIONS / ABBREVIATION o HTTPS - Stands for Hypertext Transfer Protocol Secure (HTTPS) and is a variant of standard web transfer protocols (HTTP) which adds a layer of security to data in transit o SSL - Stand for Secure Sockets Layer and is a secure protocol that protects information sent over the internet. • 4.2.1 ACCEPTABLE ENTERPRISE COMMUNICATIONS USE o Questionnaire and Survey: Microsoft Forms o Guideline for Microsoft Forms – GIT/Security Guideline/COMP&GOV/D2 o Users are responsible to ensure that collecting of personal information must be adhering to Malaysia's PDPA act and regulation. Point of references can be found in the PDPA Compliance Manual or by engaging the respective BU PDP Officers. • 4.5.6 PUBLIC FACING WEBSITES AND APPLICATIONS o Public facing websites and applications to the internet are required to follow these security controls: a) Only HTTPS connections are	GIT (Michael Louis Singh)

	allowed. b) Use only supported versions of TLS secure protocols. c) Reputable SSL certificate of authority.	

31/03/2022	<u>Added and amended the following:</u>
	• 2. SCOPE
	  ○ 2.4 Replaced management with Sunway Top Management
	• 4.6.5 Data Sharing
	  ○ Intra-Group Data Sharing Policy found within Sunway Group's PDPA Compliance Manual intends to provide guidance on the sharing of Personal Data within and across Sunway Business Units and third party which only take place if the Data Users ensure an adequate level of protection of Personal Data it processes and that such processing is in compliance with the Act.
	  ○ This Policy shall apply to all incidents of Data Sharing and shall set forth the policies and guidelines applicable to Personal Data shared within Sunway Group to ensure the effective and secure storage of Personal Data and compliance with Sunway Group's obligations under the Act in processing the Personal Data.
	  ○ Where Data Sharing within Sunway Group is necessary and is in accordance with Intra-Group Data Sharing Policy, Data Sharing should be strictly limited to only authorised employees on a "need-to-know" basis only and access to such Personal Data should be reviewed periodically.
	  ○ Each Data User shall ensure that all Personal Data is not disclosed to third parties unless such disclosure is permitted and in accordance with Sunway Group Personal Data Disclosure Policy. Each Data User shall maintain a register of disclosures to third parties, which shall also include disclosures of Personal Data made within Sunway Group.
	  ○ For more information, please refer to Sunway Group's PDPA Compliance Manual.
	• Moved section **Review** as the last section
		GIT (Michael Louis Singh)

05/08/2024	<u>Removed and amended the following:</u>	Group Cybersecurity (Michael Louis Singh)

	• 3.0 DEFINITIONS / ABBREVIATION
	  ○ AI - Artificial Intelligence (AI) refers to the capability of a machine or computer system to perform tasks that typically require human intelligence. These tasks include learning from experience, understanding language, recognizing patterns, solving problems, and making decisions.
	  ○ ChatGPT - ChatGPT is a type of artificial intelligence (AI) developed by OpenAI. It is designed to understand and generate human-like text based on the input it receives. Essentially, ChatGPT can hold conversations, answer questions, provide information, and assist with various text-based tasks by predicting the most appropriate responses using its extensive training data.
	• 4.1.4 COPYRIGHTS
	  ○ All proprietary information, including but not limited to trade secrets, copyrighted materials, and confidential business information, must be protected when using third-party AI systems e.g. ChatGPT. Users shall ensure that no proprietary information is inadvertently or intentionally disclosed to third-party AI systems without proper authorization and safeguards.
	  ○ When using third-party AI systems, Users shall comply with all applicable copyright laws and regulations. Users are prohibited from using third-party AI systems to generate, reproduce, or distribute content that infringes on the copyrights of others.
	  ○ User shall exercise caution when sharing data with third-party AI systems to prevent the unauthorized disclosure of sensitive or proprietary information. All data shared with third-party AI systems must be anonymized and de-identified to the extent possible to protect Sunway Group's intellectual property and privacy rights.
	• 4.6.2 INTELLECTUAL PROPERTY
	  ○ Any content generated using third-party AI systems that includes Sunway Group-owned information must be treated as Sunway Group property and adhere to existing policies on intellectual property. Users shall ensure that the use of third-party AI systems does not result in the unauthorized use or distribution of Sunway Group-owned copyrighted materials.	

	• 4.7 Mobile device security & Control
	  ○ 4.7.1 APPROVAL REQUIREMENT
	  ▪ Users who need to access Sunway Group information asset through mobile devices, will require the approval based upon the following:
	  • Sunway Group users – Head of Department/PCM
	  • Non-users – Business Unit Head.
	  ▪ Users are advised to have the latest Operating System and patches within the capability of their mobile devices.
	  ▪ The access to Sunway Group information asset will be granted only upon user's acceptance of this policy.
	  ○ 4.7.3 CHANGE OF MOBILE DEVICE
	  ▪ In the event users change, or no longer use the mobile device, users must inform IT Administrator immediately in order for the Sunway Group mobile applications and information asset in mobile devices to be wiped.
	  ▪ Sunway Group mobile applications and information asset in the mobile devices that are no longer in use must be wiped before granting access to the new mobile device. The purpose of performing wipe for mobile devices that are no longer in use is to protect Sunway Group information asset from the risks of being compromised.	