



Synergy House Berhad Group of Companies - Information Technology Policy



	Document Code:	Revision No.:	Revision Date:	Supercedes:	Page No. 2 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

TABLE OF CONTENTS

	Page
1. INTRODUCTION/PURPOSE	3
2. SCOPE	3
3. DEFINITION OF TERMS / ABBREVIATIONS	3
4. POLICIES	4 -18

	Document Code:	Revision No.:	Revision Date:	Supercedes:	Page No. 3 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

1. INTRODUCTION/PURPOSE

The purpose of this policy is to provide guidelines for the acceptable use of Information Technology and user to exercise basic maintenance for all IT equipment under their responsibility.


2. Scope

This policy is applicable to all Information Technology users and personnel of Synergy House Berhad Group of companies. It is the responsibility of all employees to ensure effective implementation of this procedure.

3. Definition of terms/abbreviations

The Company - Synergy House Berhad Group of Companies

IT – Information Technology

	Document Code:	Revision No.:	Revision Date:	Supercedes:	Page No. 4 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

4. Policies

4.1 Responsibility


Users of the computing and networking facilities accept the following specific responsibilities:

4.1.1 Security

- To safeguard their data, personal information, passwords and authorization codes, and confidential data.
- To take full advantage of file security mechanisms built into the computing systems.
- To choose their passwords wisely and to change them periodically.
- To follow the security policies and procedures established to control access to and use of administrative data.

4.1.2 Confidentiality

- To respect the privacy of other users. For example, not to intentionally seek information on, obtain copies of, or modify files, tapes, or passwords belonging to other users or the Company
- Not to represent others, unless authorized to do so explicitly by those users.
- Not to divulge sensitive personal data to which they have access concerning staff or users without explicit authorization to do so.
- To respect the rights of other users. For example, to comply with all Company policies regarding sexual, racial, and other forms of harassment. The Company is committed to being a racially, ethnically, and religiously heterogeneous community.
- To respect the legal protection provided by copyright and licensing of programs and data. For example not to make copies of a licensed computer program to avoid paying additional license fees or to share with other users.
- To respect the intended usage of resources. For example, to use only the account name and password, funds, transactions, data, and processes assigned by service providers, unit heads, or project directors for the purposes specified, and not to access or use other account names and passwords, funds, transactions, data, or processes unless explicitly authorized to do so by the appropriate authority.

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 5 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					


- To respect the intended usage of systems for electronic exchange (such as e-mail, World Wide Web, etc.). For example, not to send forged electronic mail, mail that will intimidate or harass other users, chain messages that can interfere with the efficiency of the system, or promotional mail for profit-making purposes. Also, not to break into another user's electronic mailbox or read someone else's electronic mail without their permission.
- To respect the integrity of the computing and networking facilities. For example, not to intentionally develop or use programs, transactions, data, or processes that harass other users or infiltrate the system or damage or alter the software or data components of a system. Alterations to any system or network software or data component are to be made only under specific instructions from authorized SYNERGY HOUSE BERHAD staff or IT Person In Charge.
- To respect the financial structure of the computing and networking facilities. For example, not to intentionally develop or use any unauthorized mechanisms to alter or avoid charges levied by the Company for computing, network and data processing services.
- To adhere to all general Company policies and procedures including, but not limited to, policies on proper use of information resources and computing and networking facilities; the acquisition, use and disposal of Company-owned computer equipment; use of telecommunications equipment; legal use of software; and legal use of administrative data.

4.2 Illegal activity

- 4.2.1 In general, it is inappropriate use to store or give access to information on the company's computing and networking facilities that could result in legal action against the company.

4.3 Objectionable material

- 4.3.1 The Company's computer and networking facilities must not be used for the transmission, obtaining possession, demonstration, advertisement, or requesting the transmission of objectionable material knowing it to be objectionable material as defined by the Malaysia Censorship Act, namely:
- A film, computer game classified RC (refused classification), or a refused publication.
 - An article that promotes crime or violence, or incites or instructs in matters of crime or violence.


	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 6 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

- An article that describes or depicts, in a manner that is likely to cause offence to a reasonable adult.
- Users of the facilities should be aware that there are severe penalties under the Act for such activities; that the police or a person authorized for the purposes of the Act may without a warrant, at any reasonable time, enter any place where the operating of a computer service is carried on and inspect any articles and records kept on the premises and may seize anything that the member reasonably suspects is connected with an offense against the Act that is found on or in the place. In addition, there are penalties for delaying, obstructing, or otherwise hindering the police or authorized person in the performance of their functions under the Act and for giving false or misleading statements including statements which are misleading through the omission of information.

4.4 Restricted Material

- 4.4.1 The Company's computing and networking facilities must not be used to transmit or make available restricted material to a minor, restricted material being defined by the **Malaysian Censorship Act** as an article that a reasonable adult, by reason of the nature of the article, or the nature or extent of references in the article, to matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting would regard as unsuitable for a minor to see, read or hear.
- 4.4.2 Users of the facilities should be aware that there are severe penalties under the Act for such activities; that the police or a person authorized for the purposes of the Act may without a warrant, at any reasonable time, enter any place where the operating of a computer service is carried on and inspect any articles and records kept on the premises and may seize anything that the member reasonably suspects is connected with an offense against the Act that is found on or in the place.
- 4.4.3 In addition, there are penalties for delaying, obstructing or otherwise hindering the police or authorized person in the performance of their functions under the Act and for giving false or misleading statements including statements which are misleading through the omission of information.


4.5 Restricted Software and Hardware

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 7 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

- 4.5.1 Users should not knowingly possess, give to another person, install on any of the computing and networking facilities or run programs or other information which could result in the violation of any Company policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers, and packet observers.
- 4.5.2 The unauthorized physical connection of monitoring devices to the computing and networking facilities which could result in the violation of company policy or applicable licenses or contracts is inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information.
- 4.5.3 Visiting personnel wishing to access the networking facilities must have authorization from an IT person in charge, who must apply to Manager for temporary access rights. Utilize password facilities will be provide to ensure that only authorized users can access the system.

4.6 Copying and Copyrights

- 4.6.1 Users of the computing and networking facilities must abide by the Company Software Copyright Act.
- 4.6.2 Respect for intellectual labour and creativity is essential, this procedure applies to works of all authors and publishers in all media. It includes respect for the right to acknowledgment and right to determine the form, manner, and terms of publication and distribution. If copyright exists, as in most situations, it includes the right to determine whether the work may be reproduced at all. Because electronic information is volatile and easily reproduced or altered, respect for the work and personal expression of others is especially critical in computing and networking environments. Viewing, listening to or using another person's information without authorization is inappropriate use of the facilities. Standards of practice apply even when this information is left unprotected.
- 4.6.3 In particular, users should be aware of and abide by the Company Software Copyright Act. Most software that resides on the computing and networking facilities is owned by the Company or third parties, and is protected by copyright and other laws, together with licenses and other contractual

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 8 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					


agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the computing and networking facilities or for distribution outside the Company; against the resale of data or programs, or the use of them for non-educational purposes or for financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization.

4.7 Harassment

- 4.7.1 Company policy prohibits discriminatory harassment. The computing and networking facilities are not to be used to libel, slander, or harass any other person. The following constitute examples of Computer Harassment:
- Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family.
 - Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated.
 - Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection).
 - The display of offensive material in any publicly accessible area is likely to violate Company harassment policy. There are materials available on the Internet and elsewhere that some members of the Company community will find offensive. One example is sexually explicit graphics. The Company cannot restrict the availability of such material, but it considers its display in a publicly accessible area to be inappropriate. Public display includes, but is not limited to, publicly accessible computer screens and printers.

4.8 Wasting Resources

- 4.8.1 It is inappropriate use to deliberately perform any act, which will impair the operation of any part of the computing and networking facilities or deny access by legitimate users to any part of them. This includes but is not limited

	Document Code:	Revision No.:	Revision Date:	Supercedes:	Page No. 9 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

to wasting resources, tampering with components or reducing the operational readiness of the facilities.


- 4.8.2 The wilful wasting of computing and networking facilities resources is inappropriate use. Wastefulness includes but is not limited to passing chain letters, wilful generation of large volumes of unnecessary printed output or disk space, wilful creation of unnecessary multiple jobs or processes, or wilful creation of heavy network traffic. In particular, the practice of wilfully using the Company's computing and networking facilities for the establishment of frivolous and unnecessary chains of communication connections is an inappropriate waste of resources.
- 4.8.3 The sending of random mailings ("junk mail") is discouraged but generally permitted in so far as such activities do not violate the other guidelines set out in this document. It is poor etiquette at best, and harassment at worst, to deliberately send unwanted mail messages to strangers. Recipients who find such junk mail objectionable should contact the sender of the mail, and request to be removed from the mailing list. If the junk mail continues, the recipient should contact the appropriate local support person.

4.9 Game Playing

4.9.1 Limited recreational game playing, that is not part of the authorized and assigned research or instructional activity, is tolerated (within the parameters of each department's rules). Company computing and network services are not to be used for extensive or competitive recreational game playing. These facilities should be utilized for work related purposes. Each individual is responsible for these facilities with ethical regard for others in the shared environment.

4.10 Commercial Use

- 4.10.1 The Company for the support of its mission provides company computing and network facilities. It is inappropriate to use the computing and networking facilities for:
- Commercial gain or placing a third party in position of commercial advantage.
 - Any non-company related activity, including non-company related communications.

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 10 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

- Commercial advertising or sponsorship except where such advertising or sponsorship is clearly related to or supports the mission of the Company or the service being provided.

4.10.2 This paragraph is not intended to restrict free speech or to restrict the Company from setting up Information servers or other services specifically designated for the purpose of fostering an "electronic community" with the wider community the Company serves.

4.11 Use of Desktop Systems


- 4.11.1 Users are responsible for the security and integrity of Company information stored on their personal computer system.
- 4.11.2 This responsibility includes making regular disk backups, controlling physical and network access to the machine, and installing and using virus protection updates.
- 4.11.3 Users should avoid storing passwords or other information that can be used to gain access to other company computing resources.
- 4.11.4 Users should not store Company passwords or any other confidential data or information on their laptop.
- 4.11.5 Networks and telecommunications services and administrative systems and services to which the company maintains connections (e.g. Internet) have established acceptable use standards. It is the user's responsibility to adhere to the standards of such networks. The Company cannot and will not extend any protection to users should they violate the policies of an external network.

4.12 Printouts

- 4.12.1 Users are responsible for the security and privacy of printouts of Company information.

4.13 Use of Electronic Mails

- 4.13.1 Electronic mail and communications facilities provided by the Company are intended for research, outreach and administrative purposes. Company rules

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 11 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

and policies, applicable laws, and acceptable use policy of the provider govern their use. Electronic mail may be used for personal communications within appropriate limits.


4.13.2 Electronic mail can be both informal like a phone call and yet irrevocable like an official memorandum. Because of this, users should explicitly recognize their responsibility for the content, dissemination and management of the messages they send. This responsibility means ensuring that messages:

- Do not contain information that is harmful to the Company or members of the Company community.
- Are courteous and polite.
- Are consistent with Company policies.
- Protect others' right to privacy and confidentiality.
- Are not used for purposes that conflict with the Company's interests.
- Contain an accurate, appropriate and informative signature.
- Do not unnecessarily or frivolously overload the email system (e.g., spamming and junk mail is not allowed).
- Manual back-up should be conducted every month.
- Each department has their external hard disk hold by managers.

4.13.3 Electronic mail containing a formal approval, authorization, delegation or handing over of responsibility must be copied to paper and filed appropriately for purposes of evidence and accountability.

4.13.4 Confidentiality and Security

- Electronic mail is inherently NOT SECURE.
- As Company networks and computers are the property of the Company, the Company retains the right to allow authorized Company officers to monitor and examine the information stored within.
- It is recommended that personal confidential material not be stored on or sent through Company equipment.
- Users must ensure the integrity of their password and abide by Company policy on password security (see the relevant section on password security).
- Sensitive confidential material should NOT be sent through the electronic mail system unless it is encrypted.
- Confidential information should be redirected only where there is a need and with the permission of the originator, where possible.

	Document Code:	Revision No.:	Revision Date:	Supercedes:	Page No. 12 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

- Users should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies.
- Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users should verify its authenticity via telephone or fax.

4.13.5 Limited Warranty

The Company takes no responsibility and provides no warranty against the non-delivery or loss of any files, messages or data nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

4.14 Data Backups

- 4.14.1 Although IT does data backup stored in servers, it is the responsibility of the individual user to backup their own data safely into Drive.


4.15 Guidelines on Passwords

4.15.1 Password Management

- Passwords should be memorized.
- Passwords belong to individuals and must **never** be shared with anyone else.
- Passwords must be changed every 6 months, or immediately if compromised.

4.15.2 Password Formation

- Password security isn't just a matter of thinking up a nice word and keeping it to you. You must choose a password, which will be difficult for someone else to guess or crack.
- We often have a tendency to forget passwords, so we choose something that has particular relevance to ourselves: the name of a loved one, our favorite car, sport, or ice cream, etc. Anyone knowing a little about us can make a list of these words and easily crack the password. All-digit passwords usually fall into this category - birth dates, and phone numbers.
- Observe the following guidelines when choosing your password:

	Document Code:	Revision No.:	Revision Date:	Supercedes:	Page No. 13 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

- i. A password should be at least 8 characters long.
- ii. Never make your password a name or something familiar, like your pet, your children, or partner. Favourite authors and foods are also guessable.
- iii. Never, under any circumstances, should your password be the same as your username or your real name.
- iv. Do not have a password consisting of a word from a dictionary. Most basic tracking programs contain over 40000 words, and plenty of variations.
- v. Choose something you can remember, that can be typed quickly and accurately and includes characters other than lowercase letters.

4.16 Users & Network Code of Practice

4.16.1 The Company for administrative purposes only provides your access to the Users Network. The Users Network is a valuable but limited resource, which must be shared with others. It is your obligation to use the facilities in an efficient, ethical, legal, and responsible manner, in accordance with the Company Policies. Grossly improper behaviors may be grounds for termination of your access or be subject to other penalties, which may apply.


4.16.2 Appropriate Electronic Behavior

Users of Internet are asked to comply with guidelines of network etiquette (netiquette). Netiquette is based on the use of good manners and common sense. Some are:

- Always acknowledge electronic mail.
- Limit your email to a single screen of text where possible.
- Do not send large files as email attachments.
- Do not use offensive language.
- Be polite to other users of the Internet.


4.16.3 Illegal Activities

- Do not download or copy software without appropriate authority or license.
- It is an offence to knowingly inject viruses into any system or engage in any other form of hacking.

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 14 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

- It is an offence to transmit material which is offensive, obscene, harassing, slanderous, damaging to the files or programs of others, or which violate any applicable law. Do not download or copy software without appropriate authority.
- Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.
- All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of Senior Executive.
- Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.
- Unless express approval from IT Person In Charge is obtained, software cannot be taken home and loaded on an employees' home computer
- Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from Manager is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the business and must be recorded on the software register by IT Person In Charge.
- Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.
- The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to IT Person In Charge for further consultation by management. The illegal duplication of software or other copyrighted works is not condoned within this business and IT Person In Charge is authorised to undertake disciplinary action where such event occurs.

4.16.4 Workplace Etiquette

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 15 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

- No food, drink or cigarettes are to be consumed in near the computer equipment.
- To switch off all IT equipment after use of before leaving the office.
- Game playing is not desirable.

4.17 Internet Conditions, Standards, and Guidelines

4.17.1 Scope

The new resources, new services, and inter-connectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this statement describes The Company official policy regarding Internet security. It applies to all Company employees, users and temporaries who use the Internet with Company computing or networking resources, as well as those who represent themselves as being connected with the company.

4.17.2 Transmission of Information – Downloading

All software downloaded from non-Company sources via the Internet must be screened with virus detection software prior to being invoked. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

4.17.3 Suspect Information


All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

4.17.4 Contacts

Contacts made over the Internet should not be trusted with Company information unless reasonable steps have been taken to ensure the legitimacy of the contacts. This applies to the release of any internal Company information.

4.17.5 Information Security

Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, Company, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.

	Document Code:	Revision No.:	Revision Date:	Supercedes:	Page No. 16 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

4.17.6 Software Security

Company computer software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-company party for any purposes other than Company purposes expressly authorized by Synergy House Berhad.

Exchanges of software and/or data between Company and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

4.17.7 Personnel Security – Privacy

Staff using Company information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers should not send information over the Internet if they consider it to be private. Any doubts regarding the privacy of information should be resolved by contacting the system’s custodian or Synergy House Berhad IT person in charge.

4.17.8 Right to Examine


At any time and without prior notice, Company management reserves the right to examine e-mail, personal file directories, and other information stored on Company computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of Company information systems.

4.17.9 Resource Usage

The Company encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not Company time. Likewise, games, news groups, and other non-Company activities must be performed on personal, not Company time. Use of Company computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no Company activity is pre-empted by personal use.

4.17.10 Public Representations

Staff may indicate their affiliation with the Company in bulletin board discussions and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address. In either case, whenever staff provide an affiliation,

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 17 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

they must also clearly indicate the opinions expressed are their own, or not necessarily those of the company.

- All staff must not publicly disclose internal Company information via the mass/electronic media or Internet that may adversely affect the Company's relations or public image.
- Staff may not establish modems, Internet or other external network connections that could allow non-Company users to gain access to company systems and/or networks and company information unless approved by Managers. Only limited personnel can access to the Internet.

4.18 Reporting Security Problems

4.18.1 Synergy House Berhad IT person in charge must be notified immediately when:


- Sensitive Company information is lost, disclosed to unauthorized parties, suspected of being lost or disclosed to unauthorized parties.
- Unauthorized use of Company information systems has taken place, or is suspected of taking place.
- There is any unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages.
- Security problems should not be discussed widely but should instead be shared on a need-to-know basis.

4.19 Questionnaires/Query

4.19.1 Any inquiry, complaint and request must be forwarded or reported to Synergy House Berhad IT person in charge.

4.20 Action

4.20.1 Violations of these computer security policies can lead to withdrawal and/or suspension of system and network privileges and/or disciplinary action. Legal or discipline action may be taken by the company Human Resource Dept if any staff is found to have breached the User Responsibility without any regard for the Company's Security Policies.

	Document Code:	Revision No.:	Revision Date:	Supersedes:	Page No. 18 of 18
	SHB-IT-2023-P02	2	25/09/2023	12/03/2021	
Information Technology Policy					

4.21 IT Procurement Policy

4.21.1 Purchasing procedure

- i. Procurement will be done by the subject matter expert.
- ii. The subject matter expert needs to obtain external consultant advice.
- iii. The amount of external consultant parties required will be based on value of the item.
- iv. Multiple quotation policy is to be applied base on the value of item purchased.

The purchase of computer systems includes notebooks, laptops, desktops and workstations. The computer systems purchased must run a Business Operating System and integrate with existing hardware. The computer systems must be purchased as standard computer system bundle and must be reputable brands.

The computer system bundle must include:

- Keyboard
- Mouse
- Charger

All purchases for computer systems must be in line with the purchasing policy in the Financial policies and procedures manual.