JENTAYU SUSTAINABLES

Information Technology Policy

JENTAYU Group of Companies

Issue No. : 1
Approved date : 25 February 2026
INTERNAL USE ONLY

INFORMATION TECHNOLOGY POLICY

Approved by the BOD of JSB
25 FEBRUARY 2026

TABLE OF CONTENT

INTRODUCTION

1. Objective

1.1. The objective of this policy is to set out the measures, standards, guidelines and procedures required to protect the Company's ICT Facilities, computer systems, equipment, information, assets, devices, and network infrastructure (collectively referred to as "ICT Systems"). These measures are designed to safeguard Jentayu Sustainables Berhad ("JSB") and its subsidiaries from internal and external threats, whether deliberate or accidental.

1.2. ICT Systems include, but are not limited to:

1.2.1. Desktop and portable computers;

1.2.2. Printers, servers, and storage devices;

1.2.3. Network and security appliances;

1.2.4. Internet, domain, and website; or

1.2.5. Email services, software, systems, and applications.

1.3. This policy serves to guide users in:

1.3.1. Protecting all ICT Systems from unauthorized access.

1.3.2. Complying with relevant Company Policies.

1.3.3. Mitigating risks through secure handling, storage, maintenance, and renewal of ICT Systems and related third-party services.

2. Definitions

JSB	Jentayu Sustainables Berhad
ITD	Information Technology Department
HOD	Head of Department
HRD	Human Resource Department
HITD	Head of IT Department
IT	Information Technology
Company	refers to Jentayu Sustainables Berhad, including its headquarters, branch offices, subsidiaries, and any entity under its operational control

Users	All employees of the Company and all third parties authorized to use the ICT Systems including, but not limited to, contractors and sub-contractors
PDPA	Personal Data Protection Act 2010
ICT System	Collectively referred to computer systems, equipment, information, assets, devices and network infrastructure
SharePoint	The subscription of Microsoft platform to store all files and/or documents in the cloud
Data subject	A living, identified, or identifiable natural person about whom the Company holds personal data
Personal data	means any information relating to a data subject who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject.

3. Scope

3.1. This policy applies to all users of ICT Systems and applications of JSB and its subsidiaries.

3.2. It covers all hardware platforms, applications, and systems used across JSB's business units, including partners, staff, and contractors.

4. Key Principles

4.1. All ICT Systems are to be protected against unauthorized access.

4.2. All ICT Systems are to be used only in compliance with relevant Company Policies.

4.3. All employees of the Company and all third parties authorized to use the ICT Systems including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this policy and must adhere to and always comply with it.

4.4. All HOD must ensure that all Users under their supervision consistently adhere to and comply with this Policy.

4.5. All data stored on ICT Systems are to be managed securely in compliance with all relevant parts of PDPA and all other existing laws governing data protection or any future regulatory requirements.

4.6. All data stored on ICT Systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data, and confidential information). All data classifieds must be handled appropriately in accordance with its classification.

4.7. All data stored on ICT Systems shall be available only to those Users with legitimate access.

4.8. All data stored on ICT Systems shall be protected against any potential of unauthorized access and/or processing.

4.9. All data stored on ICT Systems shall be protected against loss and/or corruption.

4.10. All ICT Systems are to be installed, maintained, serviced, repaired, and upgraded by the ITD or by any third party/parties appointed and authorized by the ITD from time to time.

4.11. The responsibility for the security and integrity of all ICT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the ITD unless expressly stated otherwise.

4.12. All breaches of security pertaining to the ICT Systems or any data stored thereon shall be reported and subsequently investigated by the ITD. Any breach which is either known or suspected of involvement with personal data shall be reported to HITD.

4.13. All Users must promptly report any security concerns related to the ICT Systems or the data stored within them to ITD. If the concern involves personal data in any way, it must be reported to HITD instead.

4.14. All work-related data related created or handled by Users is the property of the company. The Company reserves the right to extract, use and retrieve such data at any time without requiring the User's consent.

5. Responsibilities

5.1. HITD Responsibilities

HITD shall be responsible for the following:

5.1.1. Ensure that all ICT Systems are assessed and deemed suitable for compliance with the Company's security requirements.

5.1.2. Ensuring that IT security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the Company's senior management and reporting the outcome of such reviews to the Company's senior management.

5.1.3. Ensuring that all Users are kept aware of the requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the PDPA and the Computer Crimes Act 1997.

5.2. IT Team Responsibilities

The IT Team shall be responsible for the following:

5.2.1. Assisting all Users in understanding and complying with this Policy.

5.2.2. Providing all Users with appropriate support and training in IT security matters and use of ICT Systems.

5.2.3. Ensuring that all Users are granted levels of access to ICT Systems that are appropriate for each User, considering their job role, responsibilities, and any special security requirements.

5.2.4. Receiving and handling all reports relating to IT security matters and taking appropriate action in response.

5.2.5. Taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness.

5.2.6. Assisting HITD in monitoring all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future.

5.2.7. Ensuring that regular backups are taken of all data stored within the ICT Systems, and that such backups are stored at a suitable location onsite or offsite.

5.3. Users Responsibilities

5.3.1. All Users must at all times comply with all relevant provisions of this Policy when accessing or using the ICT Systems.

5.3.2. All Users must use the ICT Systems in accordance with Malaysian law and must not engage in any activities or purposes that may violate any current or future Malaysian legislation.

5.3.3. Users must immediately report any security-related concerns involving the ICT Systems to HITD.

5.3.4. Users must promptly notify ITD of any technical issues, including but not limited to hardware malfunctions or software errors affecting the ICT Systems.

5.3.5. Any deliberate or negligent breach of this Policy by Users will be addressed in accordance with the Company's disciplinary procedures.

6. Protecting the Company Interests

6.1. Any third-party consultants must be briefed on this policy and be required to comply accordingly when allowed to utilize any of Company ICT Systems.

6.2. The Company reserves the right to access the contents of employees' e-mail messages. All e-mail messages (sent and received) belong to the company and can be recovered and used as evidence in domestic proceedings and courts of law. The Company reserves the right to make available any e-mail messages to authorities, in accordance with the laws of the country in which the unit operates.

7. Review Cycle

7.1. The Policy is to be reviewed and revised as and when necessary to ensure that policies and procedures continue to be relevant and accurate.

7.2. ITD is responsible for establishing, updating, revising, implementing, supervising and maintaining these policies. ITD shall be assisted by designated employees in carrying out these procedures, in accordance with their respective job functions.

1. IT Administrative Policy

1.1. Usage of ICT Systems

1.1.1. ICT Systems will include the access to the internet, email services, all other computer hardware, software and peripherals.

1.1.2. JSB does not permit the usage of company ICT Systems involving (but not limited to) the following:

1.1.2.1. Sensitive and Illegal matters - actions involving materials and/or information that are political, malicious, offensive, pornographic and harassing in nature, and any materials/information, the truthfulness of which, has not been substantiated.

1.1.2.2. Violation of Copyright and Intellectual Property Rights - actions that violate the rights of other parties in relation to software licensing, intellectual property and information such as illegal software, unauthorized reproduction etc.

1.1.2.3. Unauthorized Access - accessing, allowing access, or attempting to access, the data and/or information belonging to other person(s) without express permission from the rightful owner(s) to do so such as “hacking” activities.

1.1.3. Misuse of Company Time and Resources

1.1.3.1. The primary use of the internet and e-mail facilities is for the company’s business purposes. It is permissible to use the company internet/e-mail for incidental personal purposes.

1.1.3.2. It should be noted that usage for personal matters and other usage that conflicts with the interests of JSB and actions that unnecessarily impede the performance of computer facilities such as chain letters, computer games, soliciting funds for unauthorized charitable or religious purposes and any related must be always avoided.

1.1.4. Risking the Integrity of ICT Systems

1.1.4.1. Actions that put JSB ICT Systems, and the data contained therein, at risk of corruption and failure such as transmission of computer viruses, intentional damage or whichever related threat. ICT Systems must be safeguarded against theft, damage and improper usage.

1.1.4.2. Good practices of handling the ICT Systems must be in place and consistently observed by all employees entrusted with the ICT Systems such as physical and

password protection, not disclosing passwords to other parties, back-up of important files and any other related risk.

1.1.4.3. All-important business-related e-mail messages and attachments should be saved into the appropriate external media by all the staff. It must be securely stored and filed or downloaded into external hard/secure drives.

1.2. Acquisition, use, maintenance and disposal of ICT hardware and software

1.2.1. Desktop/ Portable Computer Administration

1.2.1.1. Administrator or Super User credentials will be prohibited and only ITD has the rights for the administrator credential login. This is to eliminate unlimited access to the company's desktop/ portable computer and make changes to the Operating System or install prohibited software.

1.2.1.2. Employees need to ensure the Windows update runs automatically in the desktop/ portable computer.

1.2.1.3. Antivirus should be always activated.

1.2.1.4. Any external devices must be clean from viruses and other threats.

1.2.1.5. All desktop or portable computers provided should be well kept and maintained by the user. If the desktop or portable computer provided by ITD department was lost, stolen, or damaged under custody of the employee, the employee should immediately report to the ITD and local authorities. The ITD may seek replacement or reimbursement from the employee for the negligence that happened.

1.2.1.6. ITD will conduct the audit process for ICT assets on a yearly basis.

1.2.2. ICT Software Licensing and Hardware Warranty

1.2.2.1. Only legal and authorized copies of software are bought and used in JSB Group of companies.

1.2.2.2. ICT Software licensing and hardware warranty must be registered and renewed (if required). Warranty and license subscription must be registered.

1.2.3. Registered Domain Name and Other ICT Service Subscription

1.2.3.1. ITD must register all domain and ICT service subscriptions involved.

1.2.3.2. ITD must be aware of all domain and ICT service subscription expiry date.

1.2.3.3. ITD must renew all important ICT domain and licenses subscription if required.

1.2.4. ICT Network and System Access

1.2.4.1. ICT network and systems such as diagram, configuration, and access management information must be maintained by ITD.

1.2.4.2. ICT network information documents are to be considered as sensitive data and must not be shared with other parties without ITD permission.

1.2.5. Acquisition of ICT Products

1.2.5.1. Acquisition of ICT products is not limited to desktop or portable computer, computer peripheral and accessories, software, server system, storage, networking appliances and security appliances.

1.2.5.2. Acquisition of ICT products must be compatible with JSB environment, authorized by ITD, supported by manufacturer, distributor or/and reseller with the warranty, recorded in the ICT asset registration documents.

1.2.6. Registration of ICT Assets

1.2.6.1. Registration of ICT Assets for the new employee, especially for Desktop or Portable Computer entitlement, the request must be submitted by HRD to ITD.

1.2.6.2. ITD will arrange for an existing asset or perform requisition (if the asset is unavailable), register the asset or register the new ICT asset together with tagging and the new employee must sign the acceptance in Jentayu ICT Asset Management Form. Employees need to ensure the Windows update runs automatically in the desktop/ portable computer.

1.2.7. Return of ICT Assets Policy

1.2.7.1. Returning ICT asset by resigning employee or because of faulty, the employee needs to hand over the ICT Asset with Employee Clearance Form from HRD to ITD.

1.2.7.2. ITD needs to check whether the ICT Asset comply with Jentayu ICT Asset Management Form before approving the Employee Clearance Form. Completed Employee Clearance Form will be handed over to HRD.

1.2.8. Disposal of ICT Assets

1.2.8.1. Disposal of ICT assets apply to non-working or obsolete ICT products within the group.

1.2.8.2. Criteria for the ICT asset disposal is product obsolete, end of life (EOL) or faulty that beyond fix.

1.2.8.3. ITD will verify the ICT assets with ICT Asset Registration Form and propose to Finance Department for the disposal process.

1.2.8.4. To the employee involved, the new ICT asset registration form must be signed and acknowledged by ITD for the replacement.

1.2.9. ICT Service Agreement:

1.2.9.1. Related ICT services:

1.2.9.1.1. Provision of general ICT services.

1.2.9.1.2. Provision of network, hardware and software.

1.2.9.1.3. Repairs and maintenance of ICT equipment.

1.2.9.1.4. Provision of business software.

1.2.9.1.5. Provision of mobile phones and relevant plans.

1.2.9.2. ICT Agreements or renewal of ICT Agreements must be reviewed by ITD and Legal Department before approval request to the CFO and CEO Office as per LOA.

1.3. IT Solution Driven and IT Special Project

1.3.1. ITD or subsidiary related to the project must request and get approval from Senior Management.

1.3.2. If a subsidiary requires funding from JSB, a project presentation must be made to Senior Management, followed by approval in accordance with the Limit of Authority (LOA).

1.3.3. The procurement process for the project must adhere to the Finance procurement procedures.

1.3.4. All legal documents such as NDA, agreement etc. must be verified and endorsed by Legal. A soft copy of the stamped document must be kept at the Legal Department.

1.3.5. Memo from the CEO office or Board meeting paper for the said project must be approved.

1. IT Security Policy

1.1. Software Security Measures

1.1.1. All software in use on the ICT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and all relevant software updates, patches, fixes, and other intermediate releases will be applied at the sole discretion of the ITD. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release, falling within the remit of new software procurement and outside the scope of this provision.

1.1.2. If a security flaw (vulnerability) is identified in any software, the flaw will be addressed promptly. The software may be temporarily withdrawn from the ICT Systems until the flaw is effectively remedied. Should the security flaw affect, potentially affect, or be suspected of affecting any personal data, the ITD must be notified without delay.

1.1.3. No Users may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of HITD. Any software belonging to Users must be approved by HITD and may only be installed where that installation poses no security risk to the ICT Systems and where the installation would not breach any license agreements to which that software may be subject.

1.1.4. All software will be installed onto the ICT Systems by the ITD unless an individual User is given written permission to do so by the HITD. Such written permission must clearly state which software may be installed and on which computer(s) or device(s) it may be installed.

1.2. Anti-Virus Security Measures

1.2.1. Most ICT Systems (including all computers and servers) will be protected with suitable anti-virus, firewalls, and other suitable internet security software. All such software will be kept up to date with the latest software updates and definitions. For the latest Windows Operating Systems, the Windows Security and Windows Defender must be updated frequently by updating the Windows Operating Systems patches. The Windows Operating System version must be in version 10 and above on Users ICT Systems.

1.2.2. All ICT Systems protected by anti-virus software or Windows Security Defender will be subject to a full system scan at least once a month.

1.2.3. All physical media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred. Such virus scans shall be performed automatically or manually upon connection / insertion of media OR by the User OR by the IT Staff / HITD.

1.2.4. Users shall be permitted to transfer files using cloud storage systems only with the approval of HITD. All files downloaded from any cloud storage system must be scanned for viruses during the download process.

1.2.5. Any files being sent to third parties outside the Company, whether by email, on physical media, or by other means (e.g. shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. All email attachments are scanned automatically upon sending.

1.2.6. Where any virus is detected by a User this must be reported immediately to HITD (this rule shall apply even where the anti-virus software automatically fixes the problem). ITD shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be provided to limit disruption to the User.

1.2.7. If any virus or other malware affects, is likely to affect, or is suspected to affect any personal data, in addition to the above, the issue must be reported immediately to ITD.

1.2.8. Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Crimes Act 1997 and will be handled as appropriate under the Company's disciplinary procedures.

1.3. Hardware Security Measures

1.3.1. Wherever practical, ICT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorized Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorized access to such locations for any reason.

1.3.2. All ICT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by designated members of ITD.

1.3.3. No Users shall have access to any ICT Systems not intended for normal use by Users (including devices mentioned above) without the express permission of HITD. Under normal circumstances, whenever a problem with such ICT Systems is identified by a User, that problem must be reported to ITD. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of HITD.

1.3.4. All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locked area or locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.

1.3.5. All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended, they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to prevent such mobile devices from being left unattended at any location. If any mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment.

1.4. Access Security

1.4.1. Access privileges for all ICT Systems shall be determined based on Users' levels of authority within the Company and the requirements of their job roles. Users shall not be granted access to any ICT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.

1.4.2. All ICT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system as the ITD may deem appropriate and approve. Not all forms of biometric log-in are considered secure. Only those methods approved by ITD may be used.

1.4.3. All passwords must, where the software, computer, or device allows:

1.4.3.1. Be at least eight (8) characters long.

1.4.3.2. Contain a combination of upper- and lower-case letters, numbers and symbols.

1.4.3.3. Be changed at least every 90 days.

1.4.3.4. Be different from the previous password, other personal systems or internet banking.

1.4.3.5. Not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.); and

1.4.3.6. Be created by individual Users.

1.4.4. Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone, including HITD and the IT Staff. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to ITD and, where personal data could be accessed by an unauthorized individual.

1.4.5. If a User forgets their password, this should be reported to ITD. ITD will take the necessary steps to restore the User's access to the ICT Systems, which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the ICT Systems.

1.4.6. Users should not write down passwords if it is possible to remember them. If a User cannot remember a password, it should be stored securely (e.g. in a locked drawer or in a secure password database) and under no circumstances should passwords be left on display for others to see (e.g. by attaching a note to a computer display).

1.4.7. All ICT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate twenty (20) minutes of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).

1.4.8. All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company shall be set to lock, sleep, or similar, after twenty (20) minutes of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake, or similar.

1.4.9. Users may not use any software which may allow outside parties to access the ICT Systems without the express consent of HITD. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared up by HITD and, where such access renders personal data accessible by the outside party.

1.4.10. Users may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the Company networks subject to the approval from HITD, instructions and requirements provided by ITD governing the use of Users' own devices when connected to the Company network must always be followed. Users' use of their own devices shall be subject to, and governed by, all relevant Company Policies (including, but not limited to, this Policy) while those devices are connected to the Company network or to any other part of the ICT Systems. ITD shall reserve the right to request the immediate disconnection of any such devices without notice.

1. IT Data Protection Policy

1.1. Data Protection & Scope of Policy

1.1.1. All HOD are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

1.1.2. Any questions relating to this Policy, the Company's collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the respective HOD.

1.2. Data Protection Principles

The Data Protection Legislation sets out the following principles with which any party handling personal data must comply. All personal data must be:

1.2.1. processed lawfully, fairly, and in a transparent manner in relation to the data subject.

1.2.2. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.

1.2.3. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

1.2.4. accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

1.2.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject;

1.2.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

1.3. Adequate, relevant, and Limited Data Processing

1.3.1. Employees, agents, contractors, or other parties working on behalf of the JSB may:

1.3.1.1. collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

1.3.1.2. process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

1.4. Accuracy of Data and Keeping Data Up to Date

1.4.1. The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date.

1.4.2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out- of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

1.5. Data Retention

1.5.1. The Company shall not keep personal data for any longer than is necessary considering the purpose or purposes for which that personal data was originally collected, held, and processed.

1.5.2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

1.6. Data Backup

1.6.1. Corporate data, especially works-in-progress, should be saved to the cloud drives, as decided by the management to be the SharePoint provided by Microsoft. This is to ensure that data will be backed up when the services are backed up. Users in branch offices will do the same, via the company's Wide Area Network (WAN).

1.6.2. However, if data is saved on a local drive, then it is the responsibility of the user to back up onto storage media such as CD Read/Write disks or some type removable storage device, such as a mini hard drive, data cartridge, or solid state memory card.

1.6.3. Systems and data residing inside the systems shall be backed up automatically using the servers and storage in the company Data Centre service provider.

1.6.4. The backups must be stored in a secured manner in order for the data not to be easily accessed or stolen. It should be encrypted where possible.

1.7. Secure Processing

1.7.1. The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

1.7.2. All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

1.7.3. Data security must always be maintained by protecting the confidentiality, integrity, and availability of all personal data as follows:

1.7.3.1. only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

1.7.3.2. personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

1.7.3.3. authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

1.8. Accountability and Record-Keeping

1.8.1. The HOD is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

1.8.2. JSB shall always ensure privacy when collecting, holding, and processing of personal data.

1.8.3. All employees, agents, contractors, or other parties working on behalf of JSB shall be given appropriate notice about data protection and privacy, addressing the relevant aspects of Personal Data Protection Act 2010, this Policy, and all other applicable JSB policies.

1.9. Data Security

1.9.1. All personal data (as defined in the PDPA) collected, held, and processed by the Company will be collected, held, and processed strictly in accordance with the principles of the PDPA, the provisions of the PDPA and the Company's Data Protection Policy.

1.9.2. All Users handling data for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's Data Protection Policy at all times. In particular, the following shall apply:

1.9.2.1. All emails containing personal data must be marked "confidential".

1.9.2.2. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances.

1.9.2.3. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.

1.9.2.4. Personal data contained in the body of an email, whether sent or received, should be copied directly from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

1.9.2.5. All personal data to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked “confidential”.

1.9.2.6. Where any confidential or personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it.

1.9.3. Any enquiries related to data security should be addressed to ITD.

1.10. Data Storage Security

1.10.1. All data, and in particular personal data, should be stored securely using passwords and if possible encrypted using data encryption.

1.10.2. All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

1.10.3. All data stored electronically should be backed up frequently (2 times a year) with backups stored [onsite] AND/OR [offsite]. All backups should be encrypted using any equivalent data encryption such as Microsoft encryption or backup software encryption.

1.10.4. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise (without the formal written approval of the ITD and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary).

1.10.5. No data, and in particular personal data, should be transferred to any computer or device personally belonging to a User unless the User in question is a contractor or sub-contractor working on behalf of the Company and that User has agreed to comply fully with the Company’s Data Protection Policy and the PDPA Act.

1.10.6. When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

1.11. Data Disposal Security

1.11.1. When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

1.12. Data Breach Notification

1.12.1. All personal data breaches must be reported immediately to the Company’s HITD.

1.12.2. If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

1.12.3. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the HITD must ensure that the CFO is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

1.12.4. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 32.3) to the rights and freedoms of data subjects, the HITD must ensure that all affected data subjects are informed of the breach directly and without undue delay.

1.12.5. Data breach notifications shall include the following information:

1.12.5.1. The categories and approximate number of data subjects concerned.

1.12.5.2. The categories and approximate number of personal data records concerned.

1.12.5.3. The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained).

1.12.5.4. The likely consequences of the breach.

1.12.5.5. Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

1. IT Bring Your Own Device Policy

1.1. This policy applies to employees who work remotely or who bring their computers and/or other electronic devices, such as smartphones, mobile phones and tablets, into work. This Policy on Bringing Employees' Own Devices to Work (BYOD) is intended to protect the security and integrity of any personal data and the Company's technology infrastructure. It should be read in conjunction with the Company's Communications, Email, Internet and Social Media Policy, IT Security Policy, and Data Protection Policy.

1.2. All employees are permitted to use their own devices for work-related purposes. However, employees must agree to the terms and conditions set down in this policy in order to be able to connect their devices to the company network.

1.3. Employees Obligations

1.3.1. Acceptable Use

1.3.1.1. The employee is expected to use his or her devices in an ethical manner at all times in accordance with the Company's IT Security Policy, Communications, Email, Internet and Social Media Policy and Data Protection Policy.

1.3.1.2. The company defines acceptable use of employee's own devices as:

1.3.1.2.1. activities that directly or indirectly support the business of the Company.

1.3.1.2.2. reasonable and limited personal communication or recreation, such as reading or game playing.

1.3.1.3. Devices may not be used at any time to:

1.3.1.3.1. Store or transmit illicit materials.

1.3.1.3.2. Store or transmit proprietary information belonging to another company.

1.3.1.3.3. Harass others.

1.3.1.3.4. Engage in outside business activities.

1.3.1.4. Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, and documents.

1.3.1.5. Employees should be aware that any personal device used at work may be subject to discovery in litigation and may be used as evidence in any action against the Company.

1.3.2. Security

1.3.2.1. In order to prevent unauthorized access, devices must be password protected using a strong password.

1.3.2.2. Any device used must lock itself with a password or PIN if it is idle for five minutes.

1.3.2.3. Any device used must be capable of locking automatically if an incorrect password is entered after several attempts.

1.3.2.4. Employees must ensure that, if they transfer data, they do so via an encrypted channel e.g. a VPN.

1.3.2.5. Employees must not download unverified apps that may present a threat to the security of the information held on their devices.

1.3.2.6. Employees should not use unsecured networks.

1.3.2.7. The loss of a device used for work-related activities must be reported at the earliest opportunity to HITD.

1.3.2.8. Employees must report data breaches to HITD immediately.

1.3.3. Devices and Support

1.3.3.1. Devices must be presented to HITD for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before employees can access the network.

1.3.4. Cooperation with subject access requests

1.3.4.1. Any individual whose personal data is held by the Company has the right to make a subject access request. Consequently, the Company may have to access your device in order to retrieve any data that is held on it about the individual. You must allow the Company to access the device and carry out a search for information about an individual that may be held on the device.

1.3.5. Retention of Personal Data

1.3.5.1. Employees must not keep personal data for longer than necessary for the purpose for which it is being used, unless there is a requirement to retain it for longer in order to comply with a legal obligation.

1.3.6. Deletion of Personal Data

1.3.6.1. Employees must ensure that, if they delete information from a device, the information must be permanently deleted rather than left in the device's waste management system.

1.3.6.2. If removable media, e.g. a USB drive or CD, is used to transfer personal data, employees must ensure that the personal data is deleted after the transfer is complete.

1.3.7. End of Employment

1.3.7.1. Prior to the last day of employment with the Company, all employees must delete work-related personal data on his/her own device.

1.3.8. Third-Party Use of Devices

1.3.8.1. Employees must ensure that, in the event of friends or family using their devices, they are not able to access any work-related personal information by, for instance, password-protecting the information.

1. IT Communication, Email, Internet and Social Media Policy

1.1. Communication

1.1.1. Company Telephone System Use

1.1.1.1. The Company's telephone lines and mobile phones issued by the Company are for the exclusive use by Users working on the Company's business. Essential personal telephone calls regarding Users' domestic arrangements are acceptable, but excessive use of the Company's telephone system and/or mobile phones for personal calls is prohibited. Any personal telephone calls should be timed to cause minimal disruption to Users' work.

1.1.1.2. Users should be aware that telephone calls made and received on the Company's telephone lines and mobile phones issued by the Company may be routinely monitored to ensure customer satisfaction or to check the telephone system is not being abused.

1.1.1.3. If the Company discovers that the telephone system or a mobile phone issued by the Company has been used excessively for personal calls, this will be treated as a disciplinary matter and will be handled in accordance with the Company's disciplinary procedures.

1.1.2. Personal Mobile Phone Use

1.1.2.1. Essential personal telephone calls regarding Users' domestic arrangements are acceptable, but excessive use of Users' own mobile phones for personal communications (including, but not limited to, calls, messaging, emailing, and web browsing) is prohibited. In order to avoid disruption to others, mobile phones should be set to silent during normal working hours.

1.1.2.2. Any personal telephone calls on Users' own mobile phones should be timed to cause minimal disruption to Users' work and to colleagues working nearby.

1.2. Internet Use

1.2.1. The Company provides access to the internet for the sole purpose of business and to assist Users in the performance of their duties. However, the Company recognizes that Users may need to use the internet for personal purposes and such use is permitted provided it is reasonable and does not interfere with the User's performance of their duties. Users may be asked to justify the amount of time they have spent on the internet or the sites they have visited.

1.2.2. Users must not use the internet to gain or attempt to gain unauthorized access to computer material or private databases, including restricted areas of the Company's network. Nor must they intentionally or recklessly introduce any form of malware, spyware, virus, or other malicious software or code to the communications equipment or systems of the Company.

1.2.3. Users must not access or attempt to access any information which they know or reasonably ought to know is confidential or restricted.

1.2.4. Users must not access or use personal data online in any manner that is inconsistent with the Company's Data Protection Policy.

1.2.5. Users must not download or install any software without the express permission of ITD.

1.2.6. Users must not attempt to download, view, or otherwise retrieve illegal, pornographic, sexist, racist, offensive, or any other material which is in any way in bad taste or immoral. Users should note that even material that is legal under Malaysia law may nonetheless be insufficiently bad taste to fall within this definition. As a general rule, if any person might be offended by any content, or if that material may be a source of embarrassment to the Company or otherwise tarnish the Company's image, viewing that material will constitute a breach of this Policy. Any such attempt will constitute a disciplinary offence and in addition to internet access being reviewed, reduced, or withdrawn, may be subject to disciplinary action or dismissal.

1.2.7. Certain websites are blocked and cannot be accessed using the Company's Internet and Communication Facilities during normal business hours. If a User has a genuine and specific business need to access a blocked site, User must contact ITD.

1.3. Email Use

1.3.1. The email address with which Users are provided by the Company (ending in the suffix @jentayu-sustainables.com, @ohanahospital.com) is provided for business purposes in order to facilitate information sharing and timely communication with e.g clients, customers, supplier and colleagues. Any Company business which is conducted via email must be conducted using Company email and is under no circumstances to be conducted through any other personal email address or account.

1.3.2. Users should adopt the following points as part of best practice:

1.3.2.1. Before communicating via email, Users should satisfy themselves that it is the most suitable mode of communication, particularly where time is of the essence.

1.3.2.2. All emails should contain the appropriate business reference(s), either in the subject line or in the body of the text.

1.3.2.3. Emails should be worded appropriately and in the same professional manner as if they were a letter.

1.3.2.4. Users should be careful not to copy an email automatically to everyone copied in to the original message to which they are responding as this may result in inappropriate or unlawful disclosure of confidential information and/or personal data.

1.3.2.5. Users should take care with the content of emails, in particular avoiding incorrect or improper statements and the unauthorised inclusion of confidential information or personal data. Failure to follow this point may lead to claims for discrimination, harassment, defamation, breach of contract, breach of confidentiality, or personal data breaches.

1.3.2.6. All emails should be proof read before transmission, which includes ensuring that any attachments referred to in the text are actually attached and are correct and the intended recipients' email addresses are correct.

1.3.2.7. If an important document is transmitted via email, the sender should telephone the recipient to confirm that the document has been received in full.

1.3.2.8. All emails relating to an important file e.g contract, complaint and any important document that is needed for hard copy filing should be printed and filed in the appropriate place.

1.3.2.9. No email relating to an important file e.g contract, complaint and any important document that is needed for hard copy filing should be deleted unless a hard copy has first been printed and filed.

1.3.3. Users must not email any business document to their own or a colleague's personal web-based email accounts. Furthermore, Users must not email any business document to any recipients, (e.g clients, customers, colleagues) suppliers web-based email address unless specifically permitted to do so by the recipient.

1.3.4. Use of Company email for any personal matter is prohibited as it places additional strain on the Company's communications facilities.

1.3.5. Personal email use Users are permitted to access and use their personal email accounts during office hours only to the extent that such use is reasonable and does not interfere with the User's performance of their duties.

1.4. Social Media Use

1.4.1. General Principles

1.4.1.1. This section of this Policy addresses the use by Users of all types of social network and social media platforms including, but not limited to, Facebook, Twitter,

LinkedIn, Pinterest, Instagram, TikTok, YouTube and etc (collectively, “Social Media”).

1.4.1.2. The purpose of this part of Policy is to minimise the various risks to the Company presented by Social Media usage.

1.4.1.3. There are certain general principles that all Users should keep in mind when using Social Media for authorised work-related purposes. All Users must:

1.4.1.3.1. Use Social Media responsibly and professionally, and at all times in accordance with their duties.

1.4.1.3.2. Be mindful of what constitutes confidential, restricted, or other proprietary information and ensure that such information is never disseminated over Social Media without the express consent of the Management.

1.4.1.3.3. Be mindful of what constitutes personal data and ensure that personal data relating to the company, individual, colleague and etc is never disseminated over Social Media unless it is used in accordance with the Company’s Data Protection Policy and with expressed authority.

1.4.1.3.4. Ensure that their use of Social Media does not breach any other of the Company’s policies including, but not limited to Data Protection Policy.

1.4.1.3.5. Ensure that their use of Social Media does not breach any other laws, regulatory requirements, or other applicable rules set out by regulatory bodies and other organisations including, but not limited to, Malaysian Communications and Multimedia Commission (MCMC).

1.4.1.3.6. Ensure that they do not breach any copyright or other intellectual property rights when using Social Media.

1.4.1.3.7. Be mindful of the fact that any communication may be relied upon in court, to the advantage or detriment of the individual or the Company and conduct their use of Social Media accordingly.

1.4.1.4. If a User is unsure as to the appropriateness of a posting or other content they wish to publish, they should speak to Group IT at the earliest opportunity to seek clarification.

1.4.1.5. If a User sees any content on Social Media that disparages or otherwise reflects poorly on the Company, such content should be reported to ITD.

1.4.2. Personal Social Media Use

Users may use Social Media for personal purposes occasionally during work hours for example, during breaks provided that such usage complies with the provisions of this Policy and provided that it does not interfere with their work responsibilities or productivity.

1.4.3. Business Social Media Use

1.4.3.1. Certain Users may from time to time be required to use Social Media on behalf of the Company. Users should only do so with the authorisation of their Superior or The Management, in accordance with instructions issued by their Superior and in accordance with this Policy.

1.4.3.2. Use of Social Media for business purposes must comply with the provisions of this Policy at all times.

1.4.3.3. Users using Social Media on behalf of the Company may from time to time be required to interact with other internet users via Social Media, for example, in response to posts or enquiries regarding the Company. Unless the instructions issued to that User specifically authorise the User to respond without further approval, the User may not respond to any such communications without the prior approval of their Superior or Management. In any event, no User using Social Media on behalf of the Company should respond to such communications, with or without prior approval, without first consulting the relevant individual and/or department unless they are fully knowledgeable of the relevant topic and suitably qualified to respond.

1.4.3.4. Social Media contacts made during business are to be treated as confidential information belonging to the Company.

1.4.3.5. Before using Social Media on behalf of the Company, Users may require training to do so or may be required to demonstrate that they have already received suitable training, either from the Company or from a previous employer or other organisation.

1.5. Security

1.5.1. The integrity of the Company's business relies on the security of the Company's Internet and Communications Facilities. Users bear the responsibility of preserving the security of Company's Internet and Communications Facilities through careful and cautious use. In addition to the general provisions contained in this Policy, Users must also comply with the Company's Data Protection Policy.

1.5.2. Access to certain websites and online services via the Company's Internet and Communications Facilities is prohibited. Often the decision to block a website or service is based on potential security risks that the site or service poses. Users must not attempt to circumvent any blocks placed on any website or service by the Company.

1.5.3. Users must not download or install any software or program without the express permission of ITD.

1.5.4. Users must not delete, destroy, or otherwise modify any part of the Company's Internet and Communications Facilities (including, but not limited to, hardware and software) without the express permission of ITD.

1.5.5. Users must not share any password that they use for accessing the Company's Internet and Communications Facilities with any person, other than when it is necessary for maintenance or repairs by ITD. Where it has been necessary to share a password, the User should change the password immediately when it is no longer required by ITD. Users are reminded that it is good practice to change passwords regularly. Further guidance on passwords is contained in the Company's IT Security Policy.

1.5.6. Users must ensure that confidential information, personal data, and other sensitive information is kept secure. Workstations and screens should be locked when the User is away from the machine and hard copy files and documents should be secured when not in use.

1.5.7. If a User has been issued with a laptop, tablet, smartphone, or other mobile device, that device should be kept secure at all times, particularly when travelling. Mobile devices must be password-protected and, where more secure methods are available, such as fingerprint recognition, such methods must be used. Confidential information, personal data, and other sensitive information stored and/or accessed on a mobile device should be kept to the minimum necessary for the User to perform their duties. Users should also be aware that when using mobile devices outside of the workplace, information displayed on them may be read by unauthorised third parties, for example, in public places and on public transport.

1.5.8. Users using Company-issued mobile devices must not connect such devices to public wi-fi networks, for example, in cafes, restaurants, and on public transport without the express approval of a particular network from ITD.

1.5.9. When opening email from external sources Users must exercise caution in light of the risk malware, spyware, viruses, and other malicious software or code pose to system security. Users should always ensure that they know what an attachment is before opening it. If a User suspects that their computer has been affected by a virus they must contact ITD immediately.

1.6. Monitoring

1.6.1. To the extent permitted or required by law, the Company may monitor Users' use of the Company's Internet and Communications Facilities for its legitimate business purposes which include (but are not necessarily limited to) the following reasons:

1.6.1.1. To ensure Company policies and guidelines are followed, and standards of service are maintained.

1.6.1.2. To comply with any legal obligation.

1.6.1.3. To investigate and prevent the unauthorised use of the Company's Internet and Communications Facilities and maintain security.

1.6.1.4. If the Company suspects that a User has been viewing or sending offensive or illegal material (or material that is otherwise in violation of this Policy).

1.6.1.5. If the Company suspects that a User has been spending an excessive amount of time using the Company's Internet and Communications Facilities for personal purposes.

1.6.2. Users should be aware that all internet and email traffic data sent and received using the Company's Internet and Communications Facilities is logged, including websites visited, times of visits, and duration of visits. Any personal use of the internet will necessarily therefore be logged also. Users who wish to avoid the possibility of the Company becoming aware of any political or religious beliefs or affiliations should avoid visiting websites at work which might reveal such affiliations. By using the Company's Internet and Communications Facilities for personal use, Users are taken to consent to personal communications being logged and monitored by the Company. The Company shall ensure that any monitoring of Users' use of the Company's Internet and Communications Facilities complies with all relevant legislation including, but not limited to, the PDPA (Personal Data Protection Act) and the Human Rights Act 1998. For further information, please refer to the Company's Data Protection Policy.

1.6.3. When monitoring emails, the Company will normally restrict itself to looking at the address and heading of the emails. However, if it is considered necessary, the Company may open and read emails. Users should be aware that sensitive and confidential communications should not be sent by email because it cannot be guaranteed to be private. Users are reminded that any permitted personal emails should be marked as "personal" in the subject line.

JENTAYU ICT ASSET MANAGEMENT FORM

- ☐ **Jentayu Sustainables Berhad**
- ☐ **Power Sdn Bhd**
- ☐ **IPMUDA Buildermat Sdn Bhd**
- ☐ **IPMUDA Edar Sdn Bhd**
- ☐ **IPMUDA Utara Sdn Bhd**
- ☐ **IPMUDA Selatan Sdn Bhd Oriole**
- ☐ **IPMUDA Properties Sdn Bhd**
- ☐ **Roset Properties Sdn Bhd**
- ☐ **Ultimate Forte Sdn Bhd**
- ☐ **IPMUDA Tiles & Sanitaryware**

☐ **Others:**_____

ASET TYPE :

☐ Notebook (inclusive of power cable, backpack,mouse and headset)

☐ Desktop (Monitor, CPU, Keyboard and mouse)

☐ Others:_____

DETAILS OF ASSET

Brand & Model:_____ Serial Number :_____

Brand & Model:_____ Serial Number :_____

Brand & Model:_____ Serial Number :_____

Other Details :_____

STAFF PARTICULAR

Name (IN BLOCK LETTERS) :_____

Company/ Department :_____

Contact Number :_____(Ext)_____(H/P)

Date/ Time Collected :_____

Expected Date/ Time Returned (for temporary/ loan unit) :_____

Actual Date/ Time Returned :_____

ACKNOWLEDGE BY	**WITNESSED BY (IT use only):**
I hereby acknowledge receive/ use of the ICT loan unit notebook/ PC as listed above and agreed to the terms and condition stipulated.	
Signature :_____	Signature :_____
Name :_____	Name :_____
Date :_____	Date :_____