	TBH POLICY			
	Document No: IT-01	Revision: 1	Page No: **Cover Sheet**	Effective Date: 1 Dec 2021
	Policy Owner: IT	Verified by: Wipa U.	Approved by: Settha K.	Approved Date: 1 Dec 2021
Title: **INFORMATION TECHNOLOGY SECURITY POLICY**				

TBH POLICY

IT-01

INFORMATION TECHNOLOGY SECURITY POLICY

Originated by	Pumin Intarasri
Position	IT Staff
Date	01/12/2021

Verified by	Wipa Udompholchaicharoen
Position	IT & SAP Manager
Date	01/12/2021

Approved by	Settha Kuama	Approved by	Dilok Sae-lee	Approved by	Lee Szu Yang
Position	Financial Controller	Position	Deputy CEO	Position	Deputy CEO
Date	01/12/2021	Date	01/12/2021	Date	01/12/2021

Title: INFORMATION TECHNOLOGY SECURITY POLICY

1 PURPOSE

The purpose of this policy is to provide guidelines into the processes used to implement and maintain IT ("Information Technology") security for Teck Bee Hang Company Limited (TBH).

2 SCOPE

This document covers the use of all IT assets. It applies to all IT systems created or accessed by TBH staff and third party vendors. Company information represents any data contained in the IT systems or any TBH-created materials. TBH-created materials include emails created by TBH to perform business activities or to support management decision-making.

3 RESPONSIBILITY

3.1 It is the responsibility of the IT Department Head or his/her designate to maintain this document and ensure that the best practices are incorporated or updated in this Policy when applicable.

3.2 It is the role and responsibility of all TBH staff, including permanent, contract, and/or temporary staff, customers and third party vendors working with or within the TBH;

3.2.1 To take due cares in protecting the confidentiality, integrity and reliability of company information from unauthorized disclosure, modification, destruction and not to expose TBH information or IT systems to unnecessary risk.

3.2.2 To adhere and comply with this policy, which includes, but is not limited to, guidelines on:

- Unattended user equipment
- User ID and password use
- Internet, software, email and viruses
- Awareness of relevant legislation e.g. copyright and patent laws

3.3 Non-TBH staff that are authorized to access and use TBH's computing facilities and IT systems must comply with this Policy.

4 DOCUMENT REFERENCE

Nil.

5 EXHIBIT / FORMS

Nil.

6 TERMS AND DEFINITIONS

Nil.

7 POLICY STATEMENTS

7.1 User Password Management

Passwords are the principal means of validating a user's authority to access a computer service. Users are responsible for the use and care of their personal password. All users are advised to adopt the following guidelines for allocating and managing their passwords:

a) The use of weak passwords should be avoided. More specifically, use password which contains at least:

- One alpha character (a–z, A-Z)
- One numeric character (0-9)
- If possible, it should be at least 8 characters long

b) Passwords must be kept confidential.

c) Do not write passwords down and store them anywhere in office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

d) Avoid mirror password used on an external system. (Such as personal email account)

e) Change password at regular intervals and avoid re-using of old password if the Operating System (OS) supports it.

f) Change passwords for privileged accounts (e.g. those which access certain system utilities) frequently if the OS supports it.

g) Do not use the "Remember Password" feature of applications (for example, web browsers).

h) Any user suspecting that his/her password has have been compromised must report the incident and change all passwords.

7.2 Access Rights Management

7.2.1 Formal procedures must be used to control the allocation of access rights to prevent unauthorized computer access. The allocation and distribution of user passwords has to be securely controlled.

7.2.2 User access rights must be reviewed at regular intervals and in case of change of job or end of contract user rights must be adjusted accordingly.

7.2.3 All shared folder access request and changes must be send to IT and copy folder owner or authorized approver. The request should indicate who (to give the access right) and what folder & permission to give, request and approve via e-mail is acceptable.

7.2.4 User ID enables user's access to computer service. Users are responsible for actions/activity carried under their User ID. Hence, users are not to share accounts or passwords with friends or relatives and accounts cannot be transferred.

7.2.5 Users must follow good security practices in the selection and use of passwords. Users only use their user identity (user-ID and credentials) to access resources to which they are authorized.

7.2.6 User are not allowed to run password checkers on system password files, run network sniffers, break into other accounts, disrupt service, abuse system resources, misuse email, examine other user's files unless asked to do so by the file owner, download PC binaries, copy unlicensed software or allow other users to copy unlicensed software.

7.2.7 Exceptional case of Shared ID may be allowed due to Business or system constrain. Approval must be obtained from Department Head.

7.3 Network Access Control

Connections to network shall obtain approval from IT Department. Connection must be uniquely identified and authenticated. Users shall only be able to gain access to the services that they are authorized to use.

- Only TBH approved computer may connect to TBH Local Area Network (LAN)
- Confidential data transmitted over public network shall be encrypted.
- Users are not allowed to use Internet to gain access to any unauthorized computers.
- Gaming, gambling and any illegal activities via the Internet are strictly prohibited.
- Web content filtering is enabled in TBH Firewall. TBH reserves the right to review the filtering option from time to time.

7.4 Email

7.4.1 Email is a channel for business communication. Users are not allowed to send junk e-mails, chain letters, send or receive offensive materials. TBH reserves the right to view employee's email content.

7.4.2 Employee are not allowed to send information to personal email without approval of Department Heads.

7.4.3 Email auto forwarding to personal email is not allowed, unless approved by Department Heads.

7.5 Monitoring of System Access and Usage

Audit trails of security events shall be maintained for critical systems. Computer clocks shall be synchronized for accurate recording.

7.6 Controls against Virus and Unauthorized Software

7.6.1 Viruses

All personnel must ensure their computer is updated with latest virus definition file. If a virus is detected, follow the advice provided by the anti-virus software and report immediately to IT Department.

7.6.2 Software

- Only TBH approved software with license is allowed in user's computer.
- The IT Department should control all PC software configurations.
- Employees are not allowed to bring pirated software into TBH including software store / applications installed in their Tablet or Smartphone. Employees are liable if they violate software copyrights privacy.

7.7 IT Security Incident Management

7.7.1 Staff is responsible for the IT equipment (i.e. laptop, notebook, mobile phone, etc.) that are issued to them. They must report any loss or theft of IT equipment to their Department Head and/or IT Department within 24 hours and supported with a police report.

7.7.2 Staff should report any suspicious information security breaches to their Department Head and IT Department.

7.7.3 Staff may need to pay for the damage/loss of IT equipment, subject to management final decision.

7.7.4 Upon observation or notice of any suspected Information Security Incident, staff shall use reasonable efforts to promptly report such knowledge and/or suspicion to IT or report to the following address:

Email: it@teckbeehang.com

Or report via company website:
https://teckbeehang.com/whistleblower/#information_security

7.8 Bring Your Own Device ("BYOD")

7.8.1 The company does not encourage their employees to use their own computer. In certain circumstances, employees can use their own mobile phone/tablet for TBH email or other approved Apps.

7.8.2 Approved Apps can be installed in BYOD: TBH email, SSL VPN client.

7.8.3 Employee are responsible to ensure the BYOD that installed with approved Apps are password protected.

7.9 Security off-premises

When working at an alternate worksite away from office, adequate protection of information assets must be ensured.

7.9.1 Work from Home

Employee must comply with following guidelines:

- Treat company information (documents or data) as you would in the office.
- Do not store TBH business information in personal home computers.
- Do not share TBH business information with family members or friends.
- Do not allow TBH issued or loaned laptop to be used by family or friends.
- Use TBH laptop for TBH business purpose only.
- Ensure TBH laptop is kept secure at all time.
- Ensure up-to-date virus definition / signature file is installed on TBH laptop.

7.9.2 Business travelling guidelines

Employee should observe the guidelines while travelling with confidential and sensitive information or laptop.

- Hardcopy of information or company laptop must be carried as hand luggage and must

not be left unattended. As an additional protection, sensitive information in the hard disk should be encrypted.

- Information shall not be read, discussed or exposed in public places such as in planes, restaurants, etc.

- Employees are not to reveal their identity and TBH affiliation unnecessarily such as on luggage tag or dressing, especially when travelling with considerable proprietary information.

7.10 Responsibility of assets

7.10.1 Inventory of Assets

Each Department is responsible for maintaining their respective inventories of assets, this helps to facilitate risk assessment and effective security protection.

IT is responsible for maintaining an updated list of inventories.

7.10.2 Acceptable use of assets

All employees, contractors and external parties should follow the rules of TBH for acceptable use of information assets & physical assets associated with information processing facilities.

7.11 Physical Security

7.11.1 Office Areas

All personnel are required to use company issued access card or face scan to access TBH office. The company access card and face scan access is managed by HR Department.

7.11.2 Server Room

IT facilities supporting critical or sensitive business activities are housed in secure areas to prevent unauthorized access, damage and interference to IT services. Only authorized IT staff are allowed to access server room by using company issued access card or finger print. Head of IT Department shall review the access rights on a periodic basis.

7.12 Fire Protection

7.12.1 Fire detection or suppression systems and firefighting equipment should be provided in compliance with Fire Safety Act.

7.12.2 The amount of combustible materials (i.e. highly inflammable materials) such as paper files/documents, plastic materials, redundant computer equipment, etc. stored in the server room shall be limited.

7.12.3 Environment, Health, and Safety (EHS) department shall conduct Inspection and maintenance of fire equipment and system at least annually.

7.13 Environmental Control of Server Room

7.13.1 IT equipment shall be sited or protected to reduce the risks of damage, interference and unauthorized access. Critical business processing equipment must be protected from power failures or other electrical anomalies.

7.13.2 Power and telecommunication cabling must be protected from interception or damage.

7.13.3 Air-conditioning systems and uninterruptible power supply units shall be installed in server room.

7.13.4 There shall be no eating and drinking in the server room. The area shall be kept clean at all times

7.13.5 Inspection, testing and maintenance of the equipment and systems shall be scheduled annually.

7.14 Operation Security

7.14.1 Operational procedures and responsibilities

Procedures for the management and operation of all computers and networks must be documented to ensure the correct and secure operation of IT resources. Incident management responsibilities and procedures must be established. Proposals to use external facilities or services must identify the full security implications and include appropriate security controls.

7.14.2 External Party Management

Employees who engage in activities associated with external parties who have access to TBH Information or Information Processing Facilities, processing or maintain information on behalf of TBH, or handling of TBH information shall define security arrangements and aspects of service management.

Appropriate contractual agreement should be made with external parties.

7.14.3 System planning and acceptance

a) Capacity management

The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

b) System acceptance

Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during the development and prior to acceptance.

7.15 Backup of Business Information

Back-up copies of essential business information and software must be executed regularly and tested to ensure recovery. Computer operators will maintain a log of all work carried out. Faults must be reported with corrective action taken.

7.16 Network Management

Advanced planning and preparation are required to ensure the availability of adequate capacity and resources to minimize the risk of network systems failure. Capacity requirements shall be monitored to avoid failures due to inadequate capacity.

7.17 Operating System Access Control

Inactive end user workstations must be set to lockout, to prevent access by unauthorized persons. The recommended lockout is 15 minutes.

7.18 Application Access Control

Appropriate security controls, including audit trails, shall be designed into critical application systems to prevent loss, modification or misuse of user data in application systems.

7.19 Intellectual property rights

7.19.1 It is a TBH policy to comply with all legal obligations, and to ensure that no copyright, design right or trademark materials are copied or duplicated without the owner's consent. Copyright infringement can lead to legal action, and criminal proceedings against TBH and the individual concerned.

7.19.2 Where it is necessary to use a software product on additional equipment, licenses must be extended or additional copies purchased.

7.20 Compliance with Information Technology Security Policy

It is every employee's duty to use TBH's computer resources responsibly, professionally, ethically and lawfully. Staff violating this policy may be subjected to suspension or loss of access privileges of IT resources, as well as disciplinary action up to and including termination of employment.

8 REVIEW OF POLICY

IT Department shall review this policy at least once every 2 years or earlier as required due to changes in operating/regulatory environment, and update them to current practice.

9 REVISION HISTORY

Rev	Summary of Changes made	Verified by:	Approved by	Date
0	New Policy	Wipa U.	Settha K.	1 Dec 2019
1	7.11.1 Physical Security-Office Ares Revise from finger print to face scan 7.7.4 Information Security Incident reporting channel	Wipa U.	Settha K.	1 Dec 2021