Borneo Technical (Thailand) Limited

IT Systems Policy

Version : 1.9

Version Control

Version	Date	Author	Change Reference
1.0	5 March 2010	Thanyaphon Detsereephanit	Initial Document Creation
1.1	10 June 2010	Thanyaphon Detsereephanit	First Revised
1.2	10 January 2011	Thanyaphon Detsereephanit	Update for new E-Mail Servers
1.3	9 March 2011	Thanyaphon Detsereephanit	Add System Change Control
1.4	18 February 2013	Thanyaphon Detsereephanit	MXP to AX & add 4 policies
1.5	14 June 2014	Thanyaphon Detsereephanit	Change HSGC to BORNEO
1.6	12 April 2015	Thanyaphon Detsereephanit	Revise Purchasing Policy
1.7	5 August 2019	Thanyaphon Detsereephanit	New Servers & Move to DC
1.8	3 July 2023	Piyapong Seibudta	Update for compile ATSG v8.2
1.9	4 September 2024	Piyapong Seibudta	Review and update for FY2024

Contents

1 - General Information

1.1 Introduction

Computer information systems and networks are an integral part of business at Borneo Technical (Thailand) Limited. BORNEO has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to **Ensure IT is fully aligned and support to corporate business directions** with reasons :-

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of the Borneo.
- Maintain the unified technology standard.
- Share common technology know-how and experience.

1.2 Violations

Violations may result in disciplinary action in accordance with BORNEO company policies. Failure to observe these guidelines may result in disciplinary action by the BORNEO depending upon the type and severity of the violation, whether it causes any liability or loss to BORNEO, and/or the presence of any repeated violation(s).

1.3 Administration

The IT Department is responsible for the administration of this and relevant policies.

1.4 Contents

This document provides general information in Information Technology (IT) policy. Major topics covering various IT infrastructure will be listed in the following chapters:

- 1 – General Information
- 2 - The Internet and e-mail
- 3 - Computer viruses, ransomware and spam mails
- 4 - Access codes and passwords
- 5 - Physical security
- 6 - Remote access
- 7 - Wireless network
- 8 - Connectivity with business partners
- 9 - Copyrights and license agreements
- 10 - Software and hardware standards
- 11 - System Change Controls
- 12 - Third Party Accessing
- 13 – IT Methodology- IT Program Development and Implementation
- 14 – IT Documentation
- 15 – IT System Control and Assessment
- 16 – IT Organization

All policies/standards/guidelines related to other aspects of the IT infrastructure not covered in the list above are subject to approval by Company Director and IT Manager.

1.5 Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. Additional

specific responsibilities will be listed in individual policy documents related to various aspects.

1.5.1 Manager responsibilities

Managers and supervisors must:

- Ensure that all appropriate personnel are aware of and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

1.5.2 IT responsibilities

The IT Department must:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
- Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.
- Ensure IT standards and procedures are proper communicated to related employees.
- Perform proper assessment to ensure the above standards and procedures.

2 - The Internet and E-mail

2.1 Introduction

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is email.

2.2 Policy

Access to the Internet provides to employees, BORNEO and its customers many benefits. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect BORNEO' interests, the following guidelines have been established for using the Internet and e-mail.

All Internet services provided to external customers, business partners or the public must go through the corporate Internet gateway with appropriate security and firewall protection.

All incoming and outgoing Internet email must go through corporate email gateway for anti-virus and spam_mail checking.

Instant messaging such as Line with information stored on unsecure servers provided by external Internet parties is not allowed.

2.3 Acceptable use

Employees using the Internet are representing BORNEO. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial Web sites.
- Browse through company provided proxy server.
- Accessing databases for information as needed.
- Using e-mail for business contacts.

2.4 Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to BORNEO, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Broadcasting e-mail, i.e., sending the same message to more than 50 recipients or more than five distribution list.
- Conducting personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Access web sites that is offensive, harassing, or fraudulent.

2.5 Downloads

File downloads from the Internet are **not** permitted unless specifically authorized in writing or under guidance by the IT Department.

2.6 Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

- Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
- Be responsible for the content of all text, audio, or images that she/he places or sends over the Internet. All communications should have the employee's name attached.
- Not transmit copyrighted materials without permission.
- Know and abide by all applicable company policies dealing with security and confidentiality of company records.
- Run a virus scan on any file(s) or attachment(s) received through the Internet.
- Avoid transmission of nonpublic customer information. If it is necessary to transmit non-public information, employees are required to take reasonable steps to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.
- Avoid transmission of confidential company information. If it is necessary to transmit confidential information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

2.7 Copyright

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by BORNEO and/or legal action by the copyright owner.

2.8 E-Mail Storage Policy

To save disk space and improve overall network performance, there are size limitations for user mailbox and per individual inbound or outbound E-Mail:

- All E-Mails should be downloaded and stored at local harddisk (ie. "PST" mode)
- Maximum mailbox size at server is 100GB (ie. Pending download)
- A warning E-Mail will be issued at 90% full (ie. 90GB)
- The mailbox will be prohibited to send when it is 100% full (ie. 100GB)
- Maximum size for each single E-Mail is 20MB
- Maximum size for each E-Mail to external is 20MB
- Prohibit receive is unlimited

2.9 Monitoring

All messages created, sent, or retrieved over the Internet are the property of BORNEO and *may be regarded as public information*. BORNEO reserves the right to access the contents of any messages sent over its facilities if BORNEO believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images or in any form, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. **This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

3 - Computer viruses, ransomware and spam mails

3.1 Introduction

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

"SPAM" refers generally to the sending of unsolicited mass/bulk/junk e-mail/message/postings. Spam mail may request the recipient to perform some kind of action, e.g. go to some web site or buy some service. The message may be in the form of an e-mail but could equally be another form of an electronic message such as instant message.

3.2 Background

It is important to know that:

- Computer viruses and ransomware are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

3.3 IT responsibilities

IT Department shall:

- Set-up appropriate antivirus and anti spam gateway to prevent incoming of virus or spam emails.
- Install and maintain appropriate antivirus software on all computers.
- Respond to all virus attacks, destroy any virus detected, and document each incident.
- Respond to all spam email and suspect mail loss due to false spam alarm.

3.4 Employee responsibilities

These directives apply to all employees:

- Employees shall not knowingly introduce a computer virus or ransomware into company computers.
- Employees shall not load diskettes or any external storage device such as USB memory of an unknown origin.
- Incoming diskettes, USB memory, data CDs or DVDs shall be scanned for viruses before they are read.
- Any associate who suspects that his/her workstation has been infected by a virus shall stop all PC operation immediately, unplug the LAN cable of the computer disconnect WiFi and inform the IT Department.
- Do not open or execute any email attachment unless purpose of the attachment is known. Be aware of viruses that come as email attachment from unknown origin. Some viruses/worms will disguise themselves as a season's greetings/celebrations message.
- Users should not reply to spammers, not even to “unsubscribe,” unless the sender is legitimate.

- Users should not open or forward chain e-mail, or reveal personal information, and should never buy anything from spam mail advertisements.

4 - Access Codes and Passwords

4.1 Introduction

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

4.2 IT responsibilities

The IT Department shall be responsible for the administration of access controls to all company computer systems. The IT Department will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.

Deletions may be processed by an oral request by authorized person prior to reception of the written request. The IT Department will maintain a list of administrative access codes and passwords and keep this list in a secure area. IT will also force users to change password every 90 days.

4.3 Employee responsibilities

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID and password.
- Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they might be easily obtained.
- Will change passwords at least every 90 days.
- Should use passwords that will not be easily guessed by others. (minimum password of 8 characters)
- Combination of 2 or more of the following password such as upper, lower letters, symbols and numbers. (Complexity password enable)
- Should log out when leaving a workstation for an extended period.
- Should not share common User ID and password for computer/system access.

4.4 Supervisor's responsibility

Managers and supervisors should notify the IT Department promptly whenever an employee leaves BORNEO or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

4.5 Human resources responsibility

The HR Department will notify IT Department regarding of new staff or associate transfers and terminations as soon as possible. Involuntary terminations must be reported concurrent with the termination. Meanwhile staff movement report should be provided as monthly basis.

5 - Physical Security

5.1 Introduction

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

5.2 Employee responsibilities

The directives below apply to all employees:

- All computer storage media (e.g. external disks, CDs, DVDs, USB memory, tapes) should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
- All computer storage media (e.g. external disks, CDs, DVDs, USB memory, tapes) should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
- Critical computer equipment, e.g., ERP (Microsoft Dynamics AX) servers, E-Mail servers and file servers, must be protected by a continuous power supply (UPS). Other computer equipment should be protected by a surge suppressor in countries where domestic power supply is not stable.
- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided. No eating, drinking and smoking is allowed in the Computer Room.
- Since the IT Department is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which the IT Department has set up an initial connection.
- Employees shall not take shared portable equipment such as laptop computers out of the plant without the informed consent of their department manager. Informed consent means that the manager knows what equipment is being removed from the premises, what data is on it, and for what purpose it will be used.
- Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may occur.
- All computers or any IT equipment used by employees or visitors must go through an approval and a health check by IT Department before connecting to BORNEO network. **External parties' computer equipment (PCs / Notebooks / Tablets / Smart Phones / PDAs) are not allowed to plug in to or access to BORNEO network through a wireless connection.**
- For access to Computer Room, all users or visitors must be accompanied by authorized person from IT Department.

6 - Remote Access

6.1 Introduction

Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting company needs. The company may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

6.2 Acceptable Use

Hardware devices, software programs, and network systems purchased and provided by the company for remote access are to be used only for creating, researching, and processing company-related materials. By using the company's hardware, software and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable company policies, as well as City, State and Federal laws and regulations.

Employee's eligibility to remotely access the company's computer network will be determined by their manager.
IT services that are allowed for remote access or access outside BORNEO secured network may include :

- Email, Web Mail.
- BORNEO services such as Microsoft Dynamics AX, Sales Module, Mobile Sales.
- For security reasons, direct access to servers or files from Internet are not allowed.

6.3 Equipment & tools

The company may provide tools and equipment for remotely accessing the corporate computer network. This may include computer hardware, software, phone lines, e-mail, voicemail, connectivity to host applications, and other applicable equipment as deemed necessary.

The use of equipment and software that has been provided by the company for remotely accessing the company's computer network is limited to authorized persons and for purposes relating to company business. The company is responsible for repairing to company equipment. When the employee uses her/his own equipment (BYOD=Bring Your Own Device), the employee is responsible for maintenance and repair of equipment.

6.4 Use of personal computers and equipment

There are literally thousands of possible interactions between the software needed by the remote user and the average mix of programs on most home computers. Troubleshooting software and hardware conflicts can take hours, and can result in the need to completely reinstall of operating systems and application software to remedy for problems. For that reasons the IT Department will only provide support for equipment and software provided by the company.

The company will bear ***no*** responsibility if the installation or use of any necessary software causes system lockups, crashes, or complete or partial data loss. The employee is solely responsible for backing up data on their personal machine before beginning any company work. At its discretion, the company will disallow remote access for any employee using a personal home computer that proves incompatible, *for any reason*, or does not function properly with the company-provided software, or is being used in a production environment.

7 - Wireless Network

7.1 Introduction

Wireless networks are deployed in BORNEO warehouses and meeting rooms. Below are the standards and setup requirements for maximum security protection.

7.2 IT responsibilities

- To use the enterprise class Access Point (AP) products for better management and security control. Acceptable brands are Cisco, HP Aruba, Intermec, 3-Com, TP-Links, ZyXel., Ruijie
- In warehouse environment, All AP must activate MAC address control to prevent unauthorized wireless device connections.
- In office environment (meeting rooms), WEP encryption must be used.
- All AP setup including IPs must be documented and reported to IT Department.
- Location of coverage must be identified and proper site survey should be done and documented by vendor.

7.3 Employee responsibilities

- All wireless equipment (APs) must be purchased and installed by IT Department. Employee should not purchase or install any AP.
- Employee should not connect any wireless device to the network without it was registered and setup by IT Department.

External parties' computer equipment (PCs / notebooks / tablets / PDAs) are not allowed to attach or access to BORNEO network through a wireless connection.

8 - Connectivity with Business Partners

8.1 Introduction

Connectivity with Business Partners (BP) is for data exchange, application access or remote support. Two major connection methods are direct connection and Internet connection.

BP includes Principles, Customers or Technology Partners such as software vendors.

8.2 Direct connections

Direct connections are direct LAN-to-LAN connections. Technology may include leased line, frame relay, metro-ethernet, MPLS, FTTx, ADSL and VPN.

Requirements on security controls for direct connections are:

- Known hosts (servers) and clients (PCs) on both sides (BORNEO and BP), i.e. fixed IPs or subnets.
- Allow only agreed and designated traffic flow through the direct connection, i.e. setup default "deny all" and allow only specific IP / protocols / ports / service at routing or firewall devices
- Routing or firewall devices can be Cisco routers, Juniper firewall, Sophos firewall, Fortigate firewall.

8.3 Internet connections

Internet connections include :

- BORNEO web services provided to BPs.
- Remote access connection such as telnet / Remote Desktop / Comodo / TeamViewer / AnyDesk / pcAnywhere / VNC by BPs.
- EDI or data exchange with BPs.

Requirements on security controls for Internet connection are:

- All Internet connections must go through centralized Corporate Firewall protection.
- BPs should be responsible for the security protection on their infrastructure from where they have access BORNEO services through Internet.
- BPs should be responsible for the security protection on their equipment (PC/Notebook/Tablet) which they use for accessing BORNEO services through Internet.

Disclaimer :

- BORNEO will not guarantee or promise any service level in the Internet since there are too many intermediate parties for the connectivity.
- BPs should be liable for possible damage in our system (data & application) caused by an infected or hacked machine in BP's side (e.g. ransomware, virus, hacker, trojan)

9 - Copyrights and License Agreements

9.1 Introduction

It is BORNEO' policy to comply with all laws regarding intellectual property. BORNEO and its employees are legally bound to comply with the global and local country Copyright Act and all proprietary software license agreements. Non-compliance can expose BORNEO and the responsible employee(s) to civil and/or criminal penalties.

9.2 Scope

This directive applies to all software that is owned by BORNEO, licensed to BORNEO, or developed using BORNEO resources by employees or vendors.

9.3 IT responsibilities

The IT Department will:

- Maintain records of software licenses owned by BORNEO.
- Periodically (at least annually) scan company computers to verify that only authorized software is installed.

9.4 Employee responsibilities

Employees shall not:

- Install software unless authorized by the IT Department. Only software that is licensed to or owned by BORNEO is to be installed on BORNEO's computers.
- Copy software unless authorized by IT.
- Download software unless authorized by IT.

9.5 Civil penalties

Violations of copyright law expose BORNEO and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner.
- Profits that are attributable to the copying.
- Fines for each illegal copy.

9.6 Criminal penalties

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain" expose BORNEO and the responsible employee(s) to criminal penalties in the country violating has been committed.

10 - Software and Hardware Standards

10.1 Software

All software acquired for, or on behalf of BORNEO, or developed by company employees or contract personnel on behalf of BORNEO is and shall be deemed **company property**. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

10.1.1 IT Responsibilities

All purchasing of company software shall be centralized with the IT Department to ensure that all applications conform to corporate software standards and are purchased at the best possible price and/or with the best possible support. All requests for company software must be submitted to the budget administrator for that department for approval. The request must then be sent to the IT Department, which will then determine the standard software that best accommodates the desired request. TTTC approved supplier list is the first priority in procurement process.

10.1.2 Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on company computers. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of federal and state law. In addition to violating such laws, unauthorized duplication of software is a violation of BORNEO' software policy *(refer to "**9 - Copyrights and License Agreements**" policy)*.

10.1.3 Software standards

The following list shows the standard suite of software installed on company computers (excluding test computers) that is fully supported by the IT Department:

1. **Operating System:**
    - Microsoft Windows 10/11 Professional
2. **Office Suite:**
    - Microsoft Office 365 (with language appropriate to the local country)
    - Microsoft Office 365 (specifically for Toyota Tsusho Corporation team)
3. **Email Client:**
    - Microsoft Outlook 365
4. **Security Software:**
    - Microsoft Defender for Endpoint (MDE)
5. **Web Browsers:**
    - Google Chrome (latest version)
    - Mozilla Firefox (latest version)
    - Microsoft Edge (latest version)
6. **PDF Reader:**
    - Adobe Acrobat Reader (latest version)

During transition period (Computers replacement cycle, old dot matrix printers replacement), the following software are allowed :

- Microsoft Excel 2013 SP1 for Jet Report Tools
- Microsoft Internet Explorer 8.0 or higher

- XCitium.

All tools bundled with supported Windows and Office are allowed to use with minimal support:

- Zoom
- Imaging for Windows
- Microsoft Photo Editor (from MS Office)
- Microsoft Organization Chart (from MS Office)

The following software must be purchased and installed upon request for specific purposes:

- Microsoft Visio
- Microsoft Project
- Adobe Photoshop
- AutoCAD
- ACD System ACDSee

Employees needing software other than those programs listed above (un-listed software) must request approval from the IT Department. Each request will be considered on a case-by-case basis in conjunction with the software purchasing section of this policy. IT Department will not provide support for all un-listed software.

10.2 Hardware

All hardware devices acquired for, or on behalf of BORNEO, or developed by company employees or contract personnel on behalf of BORNEO is and shall be deemed **company property**. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

10.2.1 Purchasing / Procurement

All purchasing of company computer hardware devices shall be centralized with the IT Department to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price and/or with the best possible support. All requests for corporate computing hardware devices must be submitted to the budget administrator for that department for approval. The request must then be sent to the IT Department, which will then determine standard hardware that best accommodates the desired request. TTTC approved supplier list is the first priority in procurement process.

10.2.2 Hardware standards

The following list shows the standard hardware configuration for ***NEW*** company computers (excluding test computers) that are fully supported by the IT Department:

Desktops :

- HP / Dell desktop computers or All in one PC
- Desktops will be provided to employees who work primarily from the office
- Intel Core i5 Processor or higher
- 16GB Memory or higher
- 500GB SSD or higher with following recommendation:
    - System partition (C:): NTFS (Windows 10/11)
    - Data partition (D:): NTFS or Fat32
- Optional optical drive (DVD or CD)
- 10/100/1000 network interface card
- Video display card, at least 2 USB ports, Sound card, mouse, and all applicable

cables
- Standard 102-key English keyboard
- 15 or 17-inch LCD monitor
- At least 3-year parts and labor (on-site) warranty

Laptops
- Laptops will only be provided to employees who are required to work frequently away from the office
- HP / Dell laptop computers
- Intel Core i5 Processor or higher
- 16GB Memory or higher
- 256GB SSD or higher with following recommendation:
    - System partition (C:): NTFS (Windows 10/11)
    - Data partition (D:): NTFS or Fat32
- DVD+/-RW drive (Optional)
- 10/100/1000 network interface card
- At least 3-year parts and labor (on-site) warranty

Printers

In a Green office environment, number of individual desktop printer should be minimized. Employees will be given access to appropriate network multi-functions laser printers. In some limited cases, employees may be given local printers if deemed necessary by their department head (e.g. for the reason of printing confidential reports).

10.3 Asset Administration

All hardware devices and software programs purchased and provided to the employee by BORNEO are to be used only for creating, researching, and processing company-related e-mail, documents, presentations, and Internet materials.

Hardware devices and software programs are to be used ethically, lawfully, and appropriately at all times.

No alterations, upgrades, or modifications should be made to hardware and software purchased by BORNEO and provided to the employee, unless approved in writing by the IT department. BORNEO retains ownership of all hardware and software provided to the employee.

The employee should ensure the hardware devices and software programs provided by BORNEO are protected from theft and physical damage using reasonable precautions. For example, laptop computers, cell phones, and pagers should never be left unattended while travelling or in an unlocked vehicle.

Should an employee loss or fail to return BORNEO provided equipment and software upon termination or the request of the IT department, the employee shall pay BORNEO the current market value as determined by BORNEO. This amount shall be garnished from any remaining paychecks, reimbursement and expense checks, bonus payments, or other legal means necessary.

11 – System Change Controls

11.1 Introduction

Microsoft Dynamics AX is a core application of BORNEO Group. Therefore the system change controls are very importance to ensure the system availability and tracking all changes to the system. The goals of a change control procedure are minimize disruption to systems and services.

11.2 User Responsibilities

All change requests must be submitted via User Request Form to IT Department. The following information should be recorded in the form, such as requester, division/department, change requirement, justification and approval signature by division or department head.

11.3 IT Responsibilities

The form should be sent to IT Department and ask for IT Manager approval before development and return to user for do testing and sign acceptation and return back to IT Department before move the sources and object codes of the program to production libraries. Consequently the completion date and installation date should be signed by IT responsible person.

11.4 IT Systems/Projects Priorities

The criteria to assign and control IT System or Projects priorities are defined with these following issues from highest to lowest priority:-

- Legal requirement
- Cycle plan or Business plan (IT Roadmap)
- Productivity Improvement or cost saving
- Infrastructure related
- Management Committee set the priority for candidate projects

12 – Third Party Accessing

12.1 Introduction

Microsoft Dynamics AX is a core application of BORNEO Group. All information is company assets and used for internal purposes only. In the case of a third party ask for access to the system. Normally the third party will not be allowed to access the system unless it is approved by the Finance Controller or Managing Director.

12.2 Third Party and Employee Responsibilities

All third party and employees are not allowed to send company information to competitor companies or outside, such as customers, items, price plan, stock and finance information and etc. except approval by Finance Controller or Managing Director.

12.3 IT Responsibilities

IT Manager has a right to track third party and employees data transfer including send or receive mails when management ask for investigate the information flow.

Once the third party accessing are allowed, IT will create a temporary user account for them and specific short period of usage and disable the account immediately after period expired.

13 – IT Methodology

- For IT Program Development and Implementation

13.1 Introduction

Best practice of methodology should be applied for IT project implementation which covers following steps of process:-

- **Plan and Scope** with clearly project plan, scope, steering committee, team and roles of each member, key success factors and benefit should be identified properly and communicated to all team member through “Project Kick-off” step.
- **User Requirement Specification (URS)** to be clearly identified by process owner.
- **Analysis and Design** to deliver the “to be” system or deliverables and agreed by user.
  (conceptual design is documented and signed off)
- **Development and testing** by IT team then proceed the **User Acceptance Test (UAT)**.
- **User should sign-off the UAT** before further project go-live or deployment.
- **User training** must be addressed approximately and ensure their confidence to use new system before going live.
- **Post implementation** support should be prepared with suitable and sufficient activities.

13.2 IT Responsibilities

Both in-house and third party program development and implementation have to follow IT standard methodology.
IT manager and IT staffs to ensure :-

1. All standard steps to be processed and documented.
2. Documents including user manual are kept per IT standard documentation and filing.
3. Security control level is set up.
4. Communicate the access method to related users.

14 – IT Documentation

14.1 Introduction

IT systems, both business applications (ERP) and office systems (Microsoft Office System) are essential to all employees to do their work. IT documents, therefore, are required to be maintained and stored (filing) properly. IT documents then can be utilized to support the following

1. As user manual to interact with IT systems including how to fix the problem.
2. As user training material
3. Guide to standard processes and desk procedures.

14.2 IT Responsibilities

In general, IT to ensure all users training (user guide) documents and IT project documents including desk procedures to be stored in public shared folders or in Intranet Website for everyone in the company able to access promptly. IT also to ensure the documents are updated properly.

15 – IT System Control and Review

15.1 Introduction

All IT systems control should be verified with standard assessment and testing as regular basis. Key areas are following:-

- Hardware/Network Infrastructure Control
- Application and Development Control
- Security Control (application access control)
- Backup and Recovery Procedure
- Disaster Recovery Plan (DRP)
- Business Contingency Plan (BCP)

15.2 IT Responsibilities

IT to ensure that IT system control of the above keys areas to be implemented and documented.
IT to conduct IT system control review (with standard assessment forms) in regular basis.
IT to co-ordinate with users to do testing for BCP and DRP
IT to correct or work with users to correct false encounters.

15.3 User Responsibilities

Users are required to participate in the BCP/DRP testing in regular basis in order to ensure that DRP/BCP are working properly.

16 – IT Organization / Education

16.1 Introduction

With the purpose to provide sufficient and fully support to business operation and next directions, **the standard policy of IT human resource management** needs to be clearly identified in the following;

- **IT organization** with structure of support requirement (services) to business operation.
- Job **roles** and **responsibilities** of each position with ***competencies*** requirement
- **Development and training plan** of primary and backup roles as competencies required.
- **Successor plan** and development.

16.2 IT Responsibilities

IT manager and staffs are required to development and implement the above human resource management to IT organization.

16.3 HR Responsibilities

IT requires HR to support, concur the process.

16.4 Information Management

With the purpose to avoid information leakage, information management should be done properly depending on the confidential level

- **Confidential Information:** Is defined as any information, documents, materials, software, photographs or blueprints which relates to:
    - The Company or any of its related corporations, their employees, contractors, suppliers or consultants.
    - Any client, business partner or other contact of the Company or any of its related corporations; or
        - Any business relationship, arrangement, contract or transaction between The Company or any of its related, associated or affiliated corporations and any person, whether represented in tangible or electronic or any other form.

- **Clarification of responsibility**
  It shall establish a formal organizational structure for information security promotion and clarify the roles and responsibilities in order to protect and manage the information assets appropriately.
- **Establishment and compliance of Information security regulations**
  - The system of information security regulations (hereinafter referred to as "information security regulations") shall be "basic policy", "countermeasure standards", and "implementation procedures".
  - This policy is made as the "basic policy" of the information security regulations, and the measure standards" and "implementation procedures are formulated based on the "basic policy".
- **Risk Management**
  - It shall identify information assets to be protected and information security threats to them.
  - It shall take necessary measures to prevent the occurrence of events that impair the confidentiality, integrity, or availability of information assets (hereinafter referred to as "information security incidents") based on the status of preparation for the identified threats and the degree of impact of the threats.
  - In the event of an information security incident, it shall promptly take measures to converge the event restore to the original state, prevent the further damage, and prevent the recurrence

- **Information Classification Types:**

  <u>Classified:</u>
    - **Highly Confidential :** Information which must not be disclosed apart from where specifically specified

    - **Confidential:** Information that classified as confidential which must not be disclosed

- **Protected :** Information that in the Confidential and Internal Persons Concerned Use Only classifications which must not be disclosed to any party outside the company

Examples are as follows:

Highly Confidential	- Materials submitted to board meetings, head office managers' meetings and all company's meetings (minutes, materials for presentation), Information about the price of items, a plan of items - Non-publicized financial statements including individual detailed statements - Documents and samples received from partner companies as a result of confidential agreements signed with those partner companies - Top secret projects The other information that the head of each department recognized as "Top Secret" similar to the above
Confidential	- Documentation regarding final decisions, examination and accounting - Documentation regarding agreement (a business deal agreement, individual agreement) - Information about clients (credit, settlement) The other information that the head of each department recognized as "Confidential" similar to the above
Protected	- In-house rules, notification documents - In-house training materials - All other unofficial information that a company holds

Un-Classified:

- **Public:** Contains information that can be exposed for public viewing.

- **Handling Confidential Information:**

There has to have a management ledger or record of Confidential Information that detailed the handling of Confidential Information based on the followings:

		Highly Confidential	**Confidential**	**Protected**	**Public**
Display	displayed of classification	If possible	If possible	If possible	N/A
Distribution	Prohibit to make copies	Must	N/A	N/A	N/A
	Prohibit to make more than necessary	Must	Must	Must	N/A
Mailing / Transmission	prohibit to transmit to external (not include TTC group)	N/A	N/A	Must	N/A
	Password protect for email attached	Must	Must	N/A	N/A
	Sealed or locked package for mailing	Must	Must	N/A	N/A
Storing / Retention	Lock Environment for physical documents	Must	N/A	N/A	N/A
	Prohibit storage on PC and on external media (e.g. USB)	If possible	If possible	If possible	N/A
	Save in specific access folder in the server	Must	Must	Must	N/A

	Softcopy lock with password	Must	N/A	N/A	N/A
Disposal	Shredding of documents	Must	Must	Must	N/A

- **Confidential Information received from external party:**
  Confidential Information that has been received from an external party shall be managed by the relevant personnel within the division that received such Confidential Information.

  The rules and guidelines set out shall apply to Confidential Information received from an external party and be managed in the same manner as if the Confidential Information originated from the Company.

- **Confidential Information Control:**
  Confidential Information classification is base on rules to classify and managed by each department.

- **Data Disposal control**
  all data in Client PCs and Server will be erased and destroyed before discarding.

16.5 Education Training and Awareness Raising Objective

- With purpose to raise security awareness and encourage security improvement within the company
- Security Education: Is defined as any classes, seminars, workshops and/or training conducted by the Company for Employees, Contractors to promote the importance of information security and the adverse consequences of a breach of information security.
- Security Education:
  - The company will conduct security education by training and awareness-raising activities twice a year for the following all employee or other applicable parties and contractors (including interns and temporary staffs) to enhance their awareness on information security.

  The content of the security education should include the following topics:
  - Understanding what information security is and its importance
  - Roles and responsibilities of employees and contractors in complying with security policies, practices and procedures
  - Understanding the nature of Confidential Information and how these are classified and managed accordingly
  - Understanding how to handle security incidents (method of escalation)

Approved by :

COO(RU)..... **CCO(TH) .....**

Date:……..……. **Date:……..…….**