IT Standards and Policies

Authority	Prepared by:	Reviewed by:	Reviewed by:	Approved by:
Signature:	จตุรวิธ ไชยพิพัฒน์กิจ	Isarakul Nonthasorn		
Name:	Mr. Jaturawit Chaiphiphatthanakit	Mrs. Isarakul Nonthasorn	Ms. Thitima Nitichot	Mr. Boonchok Chungsiriporn
Designation:	Asst. HRD & IT Manager	Sr. Finance & HR Manager	QESMR	General Manager

REVISION HISTORY

Precision	Description of Change
3/5/2019	Initiate document
10/03/2025	Update Policy follow version - Aica Policy IT 2 01 - Information Security Policy v1 01 - Aica Policy IT 2 03 - IT Infra Dev and Op - v1 3 - Aica Policy IT 2 04 - Computer Use - v1 8 - Aica Policy IT 2 06 - AICA IT Standards

15.4.2013
Information Security Policy, IT 2.01

INFORMATION SECURITY POLICY

Objectives

Information is a key asset in business today. It is necessary for making decisions from strategic issues to daily operations on all levels of the company. Information security is the process of maintaining the value of information:

- Integrity – information is kept intact and not damaged in an unauthorized manner
- Availability – information is accessible to authorized users when needed
- Confidentiality – information is accessible only as authorized

Sensitive information is increasingly shared with our business partners. They are entitled to trust that efficient information security measures are in place to secure this information.

The objective is to implement and maintain information security procedures and measures based on this policy and related guidelines, to:

- Protect the investment in information assets.
- Reduce business and legal risk.
- Protect the good name of the company.

Responsibilities

Every piece of information, whether in spoken, written or electronic form, must have an ***owner***. The owner is responsible for the security of the information and

- defines the confidentiality of the information through classification
- grants authority to use the information
- determines the physical protection and security requirements

Each ***individual employee*** is responsible for handling information with care according to the guidelines originating from the owner. Any observations or suspicions of information security breaches must be reported to line management.

Line management implement and maintain security procedures and measures in practice.

IT issue and maintain guidelines to secure information stored in computers and networks.

Implementation

Information security is a process that will be enforced by the line management through administrative, physical and technical measures based on this policy and the related guidelines. Individual employee's actions will be directed through guidelines, procedures and training. This policy will come into force immediately.

Related documents

IT 2.03 IT Infrastructure Development and Operations Policy
IT 2.04 Computer Use Policy

IT Infrastructure Development and Operations Policy

Editor:	Transferred from Dynea
View by:	Adam Tan, Tan ChengPeow
Document:	IT 2.03
Creation Date:	April 15, 2013
Version:	1.3

Document Control

Change Record

Date	Author	Version	Change Reference
1.5.2001		1.0	
15.4.2013	Tan Adam	1.1	Some minor changes made based on input from review of 1.0
7.7.2015	Tan Adam	1.2	Some minor changes made based on input from review of 1.1
1.6.2024	Tan Adam	1.3	Update on Server room standard setup and Anti-virus software for non-Aica domain computers

Reviewers

Name	Position
IT:	
Tan Adam	Regional IT specialist
Management	
Tan Cheng Peow	SVP Finance

Distribution

Primary Distribution

Table of Contents

1 Purpose of this document

This policy describes principles that need to be followed when developing and operating the Aica IT infrastructure.

This document defines the minimum requirements, they can be extended by local policies or guidelines. Local documents must however not be in conflict with this document.

This document is part of a set of documents related to Information Security.

- "Information Security Policy"

For more information on standards and recommendation for IT Products, please refer to the document

- "AICA INFORMATION TECHNOLOGY STANDARDS"

For more user-focused guidelines of how to use computers and services, please refer to the document

- "COMPUTER USE POLICY"

The most current versions of all IT policies and standards documents are to be found on the corporate Intranet.

2 Target audience

All Aica personnel in the IT and business organisation who are involved in developing and/or operating the IT infrastructure.

3 The Aica global network (AICAAP)

Definition

The AICAAP is the internal communications network of Aica, today used for datacommunication but in the future also for voice. It connects sites, remote offices, home offices and external parties into a homogenous network. It is comprised of transmission lines, datacommunications hardware and software and managed network services.

Services

Following services are provided through the network to our employees.

- E-mail
- Databases

- Intranet
- Internet access
- ERP systems
- Other systems, e.g HYPERION

Development responsibilities

The responsibility to develop AICAAP is with the IT organisation. The network is developed in co-operation with the business organisation. Technical solutions are agreed in the IT managers network. The implementation takes place through the regional IT organisations.

Following criteria drive the development of the network:

- Services requested
- Security
- Cost-efficiency

These criteria have to be balanced to produce the optimal solutions for Aica.

External connections

All external connections to AICAAP must pass via a firewall. It is prohibited to have modem dial-up access points open to any hardware connected to the Aica global network. In case a modem connection is necessary e.g. to perform temporary technical maintenance, it must be activated and used only under supervision.

ALL EXTERNAL CONNECTIONS TO THE NETWORK MUST BE APPROVED BY THE REGIONAL IT MANAGER.

All remote access logins must be secured through strong authentication, like challenge-response or time-synchronous smart card token, in addition to the network level user identification, especially when using the Internet.

Network vendor policy

The objective is to have as large a part of the network as possible provided by one single vendor to benefit maximally from volume discounts. Corporate IT is globally responsible for vendor evaluation and selection. Because of the fast developing situation in the telecomms business and the fact that a given vendor is not necessarily equally strong in all parts of the world, exceptions are, however, possible, but must always be approved by the regional IT manager.

Connection types

Allowed connection types are

- Frame Relay
- Leased lines

- IP/VPN (provider's network)
- Dial-in remote access (Analogue or ISDN, ADSL)
- VPN over the public internet
  - LAN-to-LAN
  - Client-to-LAN

The technical solution for VPN over the public Internet must be managed and supported end-to-end by the network provider or internal IT.

4 Account management

User accounts

New user accounts are to be created only based on written request from the supervisor of the employee.

Only the owner of data (application, directory, etc.) can authorise access to services in the company network.

After an employee has left the company the user account has to be terminated without delay. An effective process needs to be set up to get the information from HR in time. In case of a hostile termination access to the company IT equipment and network has to be prevented immediately.

Non Aica employees must sign a Confidentiality Agreement prior to getting access to the Aica network. In the agreement they will guarantee not to use the information available to them to any other purpose than the assignment they are performing. The Site Manager/General Manager for the site/legal unit that the contractor is working for is responsible for ensuring that confidentiality agreements are signed before work starts.

Network administrator accounts

Network administrators must use dedicated accounts for tasks that require administrator privileges. Personal accounts should never be assigned administrator privileges. Site / location based administrator accounts simplify the monitoring of their use and password maintenance.

Administrator account passwords need to be changed regularly and always when someone familiar with the password leaves the company or external support personnel changes.

5 Passwords

All users must change passwords regularly, the recommended frequency is every three months. Password validation should check that the passwords are not too simple and that recent passwords are not reused.

A strong password

- Is long enough, at least 8 characters
- Does not use regular words, names, etc.
- Includes numbers and (international) special characters
- Includes upper and lower case mixed

6 Computer rooms

Servers, data communication equipment, etc. must be located in dedicated computer rooms. These premises are to be kept locked and entry is allowed only under surveillance. Consult regional IT if any of the following cannot be fulfilled.

A good computer room has:

- Lock on the door
- Server room door must be inside the IT room
- Air conditioning
- Plenty of power and network outlets
- UPS
- Fire alarm system. Fire suppression systems should be non-water based and designed to not damage computer systems.
- Preferably no windows. If there are windows, they should be blaved and strengthened.
- No water or drainpipes on top of it
- Install CCTV for additional security

7 Back-ups

All active data should be backed up daily, less critical data e.g. weekly. It is recommended that also personal files will be stored on servers to facilitate and guarantee proper back-ups. Users with laptops need to take care of back-ups using special equipment or by replicating the data to a server while logged on the network.

Back-up devices must be stored separately from the computer room in a locked, fire-resistant place, preferably a rack enclosure. It is also necessary to verify the back-up integrity regularly.

Back-up can be used e.g. in the following sequence:

- Daily (Monday-Thursday) are circulated weekly
- Weekly (Friday1-Friday4) are circulated monthly
- Monthly (taken on the last Friday of January-November) are circulated yearly
- Yearly (taken on the last Friday of December) are archived

8 Virus protection

Viruses are programs designed to make unauthorised changes to programs and data and can cause major destruction of company resources. They spread primarily through e-mail and diskettes. Therefore an anti-virus program has to be active on all workstations and Exchange e-mail servers. A mechanism is also needed to guarantee that the most recent virus data is downloaded and distributed frequently, preferably daily.

Incoming thumb drive need to be scanned for viruses before reading the content. Any user who suspects that her/his workstation has been infected by a virus must immediately power off the computer and contact PC support.

IT is responsible for setting up a working virus protection system.

Computers not join to Aica domain network must installed with an Anti-virus software (not necessary to use Aica standard anti-virus software)

9 Licenses

All software installed on the computers owned by Aica must be appropriately licensed.

The licensing of all standard software used in all workstations of the organisation is handled by IT through global or regional contracts. Software products that fall into this category are:

- Microsoft
- Virus protection software (Trend Micro)

WinZip

Employees are not allowed to install or download any software without the consent of the local IT responsible.

10 E-mail

The e-mail system of Aica is Microsoft Exchange.

E-mail accounts

All Employees have an e-mail address with the following construction:

- Firstname.lastname@Aica-ap.com

No third party e-mail addresses are allowed.

All business-related e-mail must be received and sent with the official @aica-ap.com e-mail account.

Privacy

For privacy considerations, see chapter 12

11 Internet

Right to access the Internet

As a basic company policy, Internet access is provided to all Aica employees. However, it is possible to restrict access for a single user or a group of users based on local decisions or as a consequence of abuse of the internet.

For guidelines for the personal use of the Internet, please refer to chapter 3.4 in the Computer Use Policy.

Internet access points

Internet access is controlled by IT. It is envisioned that Aica will have 3 access points to the Internet, one per region. For security reasons, no stand-alone Internet connections are allowed into AICAAP.

All connections to the Internet must pass through Aica's firewalls.

Aica web site

The corporate web site is managed by the communications department. It is not permitted to establish local websites without the approval of communications.

Corporate Communications is responsible for the layout of the company's Internet homepages. Communications also manages the publishing procedure with the content providers and safeguards that all material is in line with the company's public image. Business units and Corporate Communications produce the Internet content in co-operation.

12 Privacy

Privacy expectations

Aica is committed to respect the employees' privacy and there is no monitoring of electronic communications in general and on a regular basis. Regarding privacy, however, legislation and practises vary a lot in different countries and parts of the world. Please refer to local guidelines for more information.

Monitoring and filtering

Because of the many security risks and legal aspects in using the Internet , users must be made aware of that Aica, with the help of the Internet Service providers (ISP) may monitor the use of the internet and scan the content of the downloaded material for the following reasons:

- To protect against legal actions
- To preserve bandwidth and computer resources in general
- To define and enforce access privileges

Log information on web sites visited, files downloaded, time spent on the Internet, etc. will be saved and monitored for cost control, statistics, security and problem solving purposes.

Glossary

Aica

Legal entities of Aica Group Asia Pacific.

Computer Resources

Aica's entire computer network. Specifically, Computer Resources includes, but are not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand alone computers, laptops, software, data files, and all internal and external computer and communications networks (for example, Internet, commercial online services, value-added networks, email systems) that may be accessed directly or indirectly from our computer network.

The Computer Resources are the property of Aica and may be used only for legitimate business purposes.

Users

All employees, independent contractors, consultants, temporary workers and other persons or entities that use our Computer Resources

Users are permitted access to the Computer Resources to assist them in performance of their jobs. Use of the computer system is a privilege that may be revoked at any time. In using or accessing our Computer Resources, Users must comply with the Computer User Policy provisions.

COMPUTER USE POLICY

Editor:	Transferred from Dynea
View by:	Adam Tan, Chew TeckLiong, Tan ChengPeow
Document:	IT 2.04
Creation Date:	20 Jan , 2016
Version:	1.7

Document Control

Change Record

Date	Author	Version	Change Reference
1.5.2001	.	1.0	
1.6.2001	.	1.1	Some minor changes made based on input from review of 1.0
20.1.2016		1.5	Changes made to Hardware section 7 and Passwords section 9
6.7.2017		1.6	Add Hardware replacement standard to Hardware section 7
29.8.2020	Tan Cheng Peow	1.7	Include Personal Data protection act to Privacy expectation section 4
9.5.2023	Adam Tan	1.8	Minor changes to Hardware section 7 on external hard disks, USB memory sticks, etc.

Reviewers

Name	Position
IT:	

Distribution

All Aica employees

Table of Contents

1 Purpose of this document

Aica relies on its computer network to conduct its business. To ensure that its employees, independent contractors, agents, and other computer users use its computer resources properly, Aica has created this Computer Use Policy (the "Policy").

The rules and obligations described in this Policy apply to all users (the "Users") of Aica's computer network, wherever they may be located. Violations will be taken very seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

It is every employee's duty to use Aica's computer resources responsibly, professionally, ethically, and lawfully.

This document is part of a set of documents related to Information Security.

- "Information Security Policy" (IT 2.01)

For more information on standards and recommendation for IT Products, please refer to the document

- "AICA INFORMATION TECHNOLOGY STANDARDS" (IT 2.06)

For more general guidelines for the development of The Aica IT infrastructure please refer to the document

- "IT INFRASTRUCTURE DEVELOPMENT AND OPERATION POLICY" (IT 2.03)

The most current versions of all IT policies and standards documents are to be found on the corporate Intranet.

2 Target audience

All Aica employees.

3 General principles

3.1 Company property

As a general principle, all employees have access to the Aica network and are able to use the services provided over the network.

As a company, Aica encourages the business use of IT in general as a productivity enhancement tool and electronic communication systems in particular to facilitate communication and collaboration across regions.

All business systems including their data, all electronic communications systems and all messages generated on or handled by these systems, including back-up copies, are considered to be the property of Aica.

3.2 User privileges and responsibilities

User privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted ("need-to-know"-approach).

Users may not read, alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another user does not imply permission to read, alter, or copy that file. Users may not use

the computer system to 'snoop" or pry into the affairs of other users by reviewing their files and email.

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess. See password guidelines in chapter 9.

3.3 Prohibited activities

Inappropriate or unlawful material

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by email or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in Aica's computers. Users encountering or receiving this kind of material should immediately inform the sender to discontinue sending such material and take you off the distribution lists as well as report the incident to their supervisors.

Waste of computer resources.

Users may not deliberately perform acts that waste Computer Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time online on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents through network printers, or otherwise creating unnecessary network traffic. Dial-Up access should always be used for "Send and Receive" operations only and not for synchronization or working online.

Misuse of software.

Without prior written authorization from IT, users may not do any of the following: (1) copy software for use on their home computers; (2) provide copies of software to any independent contractors or clients of Aica or to any third person; (3) install software on any of Aica's workstations or servers; (4) download any software from the Internet or other online service to any of Aica's workstations or servers; (5) modify, revise, transform, recast, or adapt any software; or (6) reverse engineer, disassemble, or decompile any software. Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

Communication of trade secrets.

Unless expressly authorized by a Senior Vice President, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the company to external business partners is strictly prohibited. Unauthorized dissemination of this Information may result in substantial civil liability as well as severe criminal penalties under any local or regional statutes.

3.4 Personal use

Aica provides the hardware and software tools and network access to email and Internet for Company purposes. It is expected that there will be a certain level of incidental personal use of these resources and that this will be primarily during non-working hours and will not violate any section of this Policy.

Incidental personal use is permissible so long as:

- It does not consume more than a trivial amount of resources

- It does not interfere with staff productivity.
- It does not preempt any business activity.

Personal use is subject to a review from time to time by Aica and the individuals' supervisor. Aica's computer resources are not to be used for any business activities outside of Aica business.

4 Privacy expectation

Aica is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

However, Aica is also responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

Privacy legislation varies from country to country. Therefore, these matters are always to be handled within the framework of national privacy legislation.

Please consult your regional IT manager and in the case of Singapore, we are required to comply to the Personal Data Protection Act (PDPA) and should you require more information on the PDPA Act, you may refer to this website https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act.

If you have any queries or feedback on our data protection policies and procedures, and our privacy statement, please contact our Data Protection Officer at dpo.singapore@aica-ap.com

No guaranteed message privacy

Aica cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

Regular message monitoring

It is the policy of Aica NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored, and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that Aica may from time to time examine the content of electronic communications.

IT staff will monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems.

Incidental disclosure

It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution. IT staff may, however, not review the content of an individual employee's communications out of personal curiosity or without being specifically authorized to do it by executive management.

5 E-mail use

E-mail accounts

All Employees have an e-mail address with the following construction:

- Firstname.lastname@Aica-ap.com

No third party e-mail addresses are allowed.

All business-related e-mail must be received and sent with the official @aica-ap.com e-mail account.

User back-ups

If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information or has value as evidence of Aica's management decisions, it should be retained for future reference. Most messages don't fall into this category and accordingly, can be erased after receipt. Users must regularly move important information from the inbox to personal folders and other archiving files. E-mail systems are not intended for the archival storage of important information. Important messages can mistakenly be erased by users, systems administators or otherwise lost when systems problems occur.

Purging electronic messages

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. It is recommended that after a certain period – generally six months – electronic messages backed up to a separate data storage media (tape, disk, CD-ROM, etc.) will be automatically deleted by IT staff.

6 Internet use

Connecting to the Internet

Employees will be provided with access to the Internet to assist them in performing their job. Confidential business information is some of the Aica's most valuable assets. Anytime an outside communication connection is made Aica's information is at risk. The Internet can pose potential risks to Aica and we must proceed accordingly. All employees or any site that requires access to the Internet must work with the Aica IT department in order to obtain access. To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to Aica's network must do so through an approved Internet firewall (check with IT for access). Accessing the Internet directly, by modem or any other technology is strictly prohibited unless the computer you are using is not connected to the company's network.

Management

The Internet has a wealth of information for the marketer, researcher, technical staff or others. It is also easy to "surf"(use) the Internet for hours without being productive. Managers of employees who access the Internet must be aware of this potential for abuse.

Most notably, surfing on following categories of internet sites is considered to be abusive use: Adult Entertainment, Pornography, Drugs, Racism, Violence, Gambling, Games and Chat Groups.

Employee's who access the Internet must be counseled and managed so that the maximum business benefit is obtained. It is the obligation of every Aica Manager to see that his/her subordinates do not abuse the use of the Internet. Users are obliged to report all observations or suspicions of Internet abuse to Management. Use of the Internet should be undertaken according to good practice, in compliance with the law, good manners, and the shared values of Aica. All copyrights pertaining to material copied from the network must be respected. The Internet should be used only for retrieving work-related information during working hours. Other information gathering must take place outside working hours, and may be entirely prohibited (at the discretion of the employee's supervisor).

Disclaimer of liability for use of Internet

Aica is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an email address on the Internet may lead to receipt of unsolicited email containing offensive content. Users accessing the Internet do so at their own risk.

7 Hardware

All computer hardware devices purchased for company employees or contract personnel on behalf of the company is and shall be deemed company property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

Purchasing and Asset Management

All purchasing of company computer hardware devices shall be centralized with regional or local IT or one person/site who controls all computing equipment purchases to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price.

Hardware standards

For hardware standards, please refer to the standards document ("AICA INFORMATION TECHNOLOGY STANDARDS" (IT 2.06))

Employees needing computer hardware different from the standard should always discuss their requirements with regional or local IT to make sure that the equipment complies with corporate standards.

Hardware replacement

Replacement with a new Desktops/notebooks should only be considered under the following circumstances : -

a) IT department has assessed the condition of the machine to be beyond economical repair
b) On a need basis; upgrade should be considered first before purchasing a new machine
c) Expiry of warranty period is not a key consideration for change when machine is still in good working condition;

Laptops and notebooks

As portable PCs are much more exposed to external crime than workstations, special security measures are required. All portable PCs shall be installed with anti- virus and encryption software and all data stored on portables shall be encrypted and scanned.

All purchases of portable PCs shall include finger print recognition as one of the specifications and access to portable PCs shall be by finger print recognition. For older portable PCs with no finger print feature, password login shall be used.

Other things to remember when traveling with a computer:

- Do not leave the portable unattended in a car
- Treat the portable as your other valuables; e.g. lock it in a hotel safe when possible
- Carry portable in your hand baggage
- Update virus protection regularly
- Back up the portable regularly

External hard disks, USB memory sticks, etc

- Only Aica approved and issued external devices such as USB, portable hard disk can be connected to Aica Laptops and Desktop computers. Users are required to scan these devices for viruses before connecting to Aica computers.
- No external devices from 3rd parties (clients, customers, and supplier) memory equipment shall be connected to Aica computers.

8 Software

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

Purchasing

All purchasing of software shall be centralized with regional or local IT or one person/site who controls all computing equipment purchases to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price.

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 is prohibited. In addition to violating licensing agreements, unauthorized duplication of software is a violation of the company's Software/Hardware Policy.

Software standards

For software standards, please refer to the standards document ("AICA INFORMATION TECHNOLOGY STANDARDS" (IT 2.06))

Employees needing computer software different from the standard should discuss their requirements with regional or local IT to make sure that the software complies with corporate standards and does not have any adverse effects on standard software.

9 Passwords and protection of Information

Responsibility

Users are responsible for safeguarding their passwords for access to the computer system and files stored with passwords protection. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system with another User's password or account.

It is prohibited to reveal a personal password to anyone, especially over the phone or e-mail. When a support technician needs to use a personal password, that must happen under surveillance and the password has to be changed immediately afterwards.

If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms.

Procedure

All users must change passwords regularly, the recommended frequency is every four months. Password validation should check that the passwords are not too simple and that recent passwords are not reused. A strong password:

- Is long enough, at least 8 characters
- Does not use regular words, names, etc.
- Includes numbers and (international) special characters
- Includes upper and lower case mixed

Protection of information stored in computers and memory devices

All users should use their best endeavor to protect confidential information such as product formulation, information of customers, pricing of products, etc stored in Aica computers and memory devices.

All users shall therefore stored all such confidential information **especially from customer** with password protection. This is to avoid leakage of such information to non intended users which may cause problem to Aica.

10 Virus protection

Viruses can cause substantial damage to computer systems. The Aica IT department will provide each computer with virus detection software. However, each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into Aica's network. To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to Aica MUST be scanned for viruses and other destructive programs. Users should understand that their home computers and laptops might contain viruses. All disks transferred from these computers to Aica's network MUST be scanned for viruses.

Glossary

Aica

Legal entities of Aica Group worldwide.

Computer Resources

Aica's entire computer network. Specifically, Computer Resources includes, but are not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand alone computers, laptops, software, data files, and all internal and external computer and communications networks (for example, Internet, commercial online services, value-added networks, email systems) that may be accessed directly or indirectly from our computer network.

The Computer Resources are the property of Aica and may be used only for legitimate business purposes.

Users

All employees, independent contractors, consultants, temporary workers and other persons or entities that use our Computer Resources.

Users are permitted access to the Computer Resources to assist them in performance of their jobs. Use of the computer system is a privilege that may be revoked at any time. In using or accessing our Computer Resources, Users must comply with the Computer User Policy provisions.

IT INFRASTRUCTURE
AICA IT STANDARDS

Author: Chew Teck Liong

Document: IT 2.06
Creation Date: April 15, 2013
Version: 1.0

Document Control

Change Record

Date	Author	Version	Change Reference
April 15, 2013	Chew Teck Liong	1.0	
June 13, 2022	Adam Tan	1.1	Disaster recovery
June 26, 2023	Adam Tan	1.2	Server Operating System

Reviewers

Name	Position

Distribution

Table of Contents

1 Purpose of this document

This document outlines the standards and practices that need to be followed when operating within the Aica IT infrastructure.

This document defines the minimum requirements to be implemented. Local policies or guidelines can extend requirements. Local documents must however not be in conflict with this document.

Adherence to this document will ensure compatibility and operability between the various entities within the Aica group.

Implementation of the contents of this document should be implemented when new sites or locations are integrated into the Aica environment. Implementation in existing sites should be phased. The intention is not to burden locations with extra costs.

2 Principles

Corporate IT unit is responsible for the active development and monitoring of the IT architecture and standards in the Aica Group. The standards are developed and set in partnership with business management and the global Aica IT team. Finally the Group Management must approve the standards.

Comments concerning this document should be addressed to the corporate IT Vice-President.

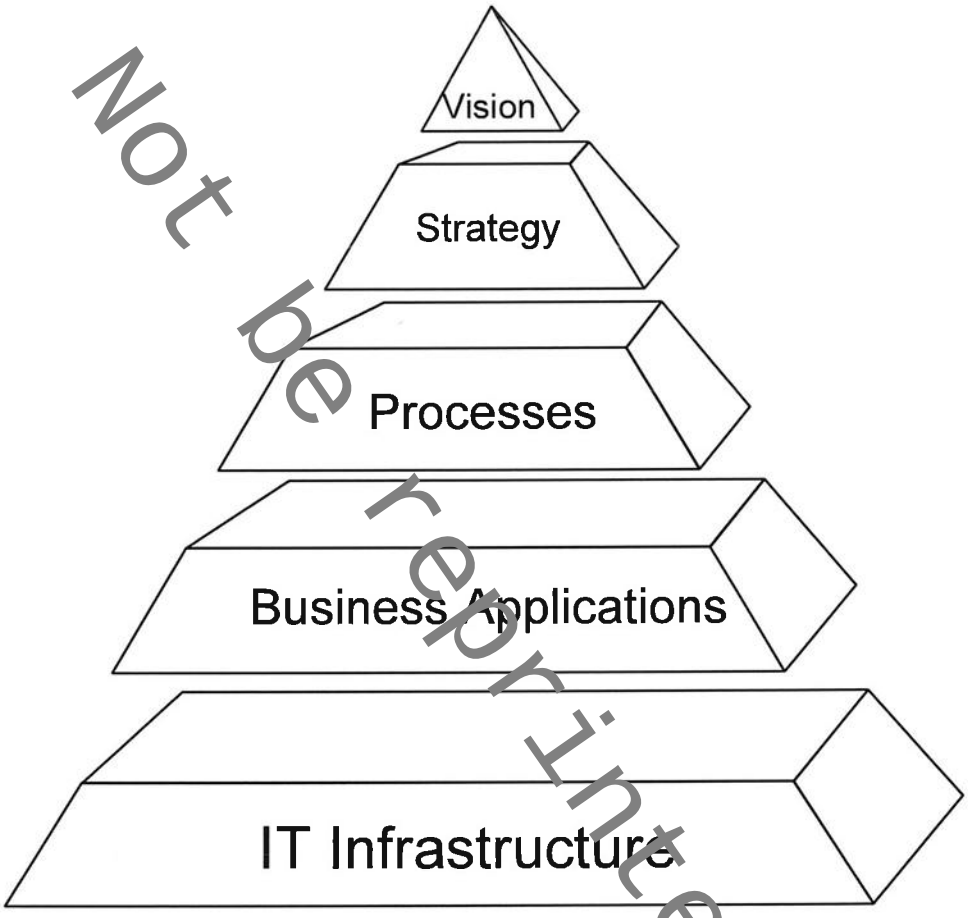
3 Target audience

All Aica personnel in the IT and business organisation who are involved in developing and/or operating the IT infrastructure.

4 What is Infrastructure?

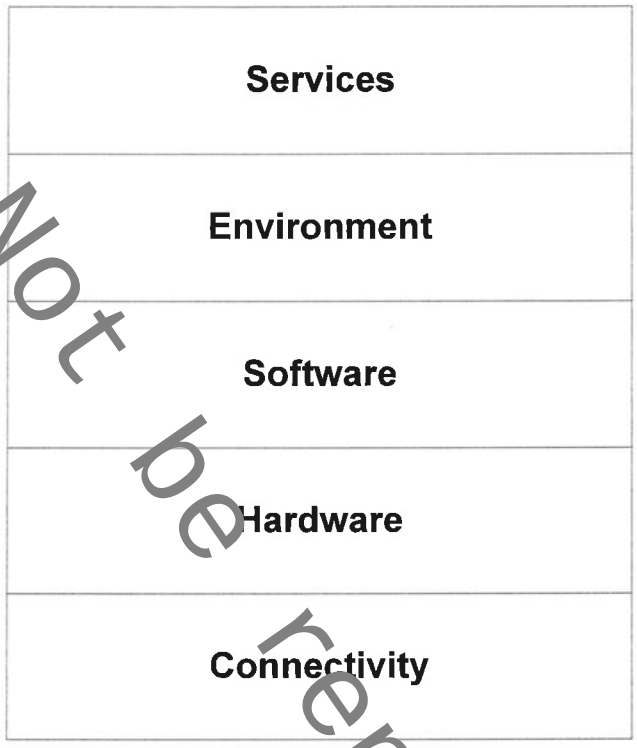
3.1 Definition

IT Infrastructure underpins the modern Business Model through connectivity and standardisation at the lowest level. If we use a plumbing metaphor, it contains the pipes, values, flow rates, pressures, pipe sizes... etc. In the IT world it covers the Cabling, Routers, Servers, Workstations, Operating Systems, Software, Protocols, etc.



5 Infrastructure

Infrastructure can be further layered into the following:



4.1 Connectivity

Connectivity can be considered the "plumbing" of the organisation. This covers what protocols, cabling, access methods, etc are to be used within the Aica group.

4.2 Hardware

Hardware covers the physical equipment that is to be used within the Aica Group. This covers such things as Servers, PC's, Printers, Routers, Switches, Hubs… etc.

4.3 Software

Software covers the programs and applications that are to be used with the Aica group. It coverts what Operating Systems, Office Automation Tools (word processing, Spreadsheets etc), Anti-Virus, Compression programs and so on are permitted.

4.4 Environment

Environment sets out the framework on how certain issues are addressed within the group. This covers such things as Naming Conventions, NT Domain pratices, security, operating environment etc…

4.5 Services

Services cover common group services such as EMail, Intranet and Internet use.

6 Structure of the Standards Documents

Each standard is numbered according to the following convention:

2.06 This document

- 2.06.1 Connectivity
- 2.06.2 Hardware
- 2.06.3 Software
- 2.06.4 Environment
- 2.06.5 Services

Under each sub-document there will be documents related to a certain sub-section, for example, under connectivity there is a 2.06.1.1 which covers protocol issues. For instance, 2.06.1.1.1 defines what protocol is to be used on the Aica network.

Documents are further divided into following sections:

Policy - This is the direction that must be followed. This is obligatory.

Guidelines - These are pointers on how to work within the policy statement.

Recommendations - These are corporate recommendations.

Convention - Descriptive

7 Standards Documents

This is a list of current documents in place:

Number	**Area**	Document Title
2.06	**IT Standards**	Aica IT Standards
2.06.1	**Connectivity**	
2.06.1.1	**Protocol**	
2.06.1.1.1		Protocol
2.06.1.1.2		IP Address Allocation
2.06.1.1.3		IP Address Structure
2.06.1.1.4		DHCP

2.06.1.2	**Cabling**	
2.06.1.2.1		LAN Cabling
2.06.1.2.2		EIA-TIA 568A
2.06.1.2.3		Connectors
2.06.1.2.4		Cabling between buildings
2.06.1.3	**WAN**	
2.06.1.3.1		WAN
2.06.1.4	**LAN**	
2.06.1.4.1		Network Access ISO Layer 2
2.06.1.4.2		Sizing LANS
2.06.1.5	**Telecommunication**	
2.06.1.5.1		PABX
2.06.1.6	**Remote Access**	
2.06.1.6.1		Remote User
2.06.1.6.2		Dial-Up Access
2.06.1.6.3		Home PC's
2.06.1.6.4		VPN over Internet
2.06.2	**Hardware**	
2.06.2.1	**Servers**	
2.06.2.1.1		PC Server Manufacturer
2.06.2.1.2		PC Server Processor
2.06.2.1.3		UNIX Server Manufacturer
2.06.2.2	**Desktop PC**	
2.06.2.2.1		PC Desktop Manufacturer
2.06.2.2.2		PC Desktop Processor
2.06.2.3	**Laptop**	
2.06.2.3.1		PC Laptop Manufacturer
2.06.2.3.2		PC Laptop Processor

2.06.2.4	**Tab's**	
2.06.2.4.1		PDA
2.06.2.5	**Printers**	
2.06.2.5.1		Network Black & White Lasers
2.06.2.5.2		Network Colour
2.06.2.5.3		Local Printers
2.06.2.6	**Network**	
2.06.2.6.1		PC Network Cards
2.06.2.6.2		Printer Network Cards
2.06.2.6.3		Laptop Network Cards
2.06.2.6.4		Routers
2.06.2.6.5		Switches
2.06.2.6.6		Hubs
2.06.2.7	**Backup**	
2.06.2.7.1		Backup Devices
2.06.2.7.2		Disaster Recovery
2.06.3	**Software**	
2.06.3.1	**Operating Systems**	
2.06.3.1.1		PC Operating Systems
2.06.3.1.2		Server Operating Systems
2.06.3.2	**Database**	
2.06.3.2.1		Large-Scale Applications
2.06.3.2.2		Mid-Size Applications
2.06.3.2.3		Small-size Applications
2.06.3.2.4		Lotus Notes
2.06.3.3	**ERP**	
2.06.3.3.1		ERP
2.06.3.4	**Office Automation**	

2.06.3.4.1		Office
2.06.3.4.2		Web Browser
2.06.3.5	**Virus Protection**	
2.06.3.5.1		EMail
2.06.3.5.2		Workstations
2.06.3.5.3		Servers
2.06.3.6	**Backup**	
2.06.3.6.1		Server
2.06.3.7	**Other**	
2.06.3.7.1		Adobe Acrobat Reader
2.06.3.7.2		Compression
2.06.4	**Environment**	
2.06.4.1	**Language**	
2.06.4.1.1		Language
2.06.4.2	**Naming Conventions**	
2.06.4.2.1		Naming Conventions
2.06.4.2.2		User Id's
2.06.4.2.3		Computer Equipment Names
2.06.4.2.4		Site Names
2.06.4.2.5		Organisation Names
2.06.4.3	**NT Domain**	
2.06.4.3.1		Domain Model
2.06.4.3.2		User Accounts
2.06.4.3.3		Drive Mappings
2.06.4.4	**Operating Environment**	
2.06.4.5	**Security**	
2.06.4.5.1		Network Access
2.06.4.5.2		Passwords

2.06.4.5.3		Laptops
2.06.4.5.4		Data Center
2.06.4.6	**Development**	
2.06.4.6.1		Development
2.06.4.7	**Asset Management**	
2.06.4.7.1		Assets
2.06.4.7.2		Software
2.06.4.7.3		Network
2.06.4.8	**Backup**	
2.06.4.8.1		Backup
2.06.5	**Services**	
2.06.5.1	**EMail**	
2.06.5.1.1		EMail
2.06.5.1.2		EMail Platform
2.06.5.2	**Internet**	
2.06.5.3	**Intranet**	
2.06.5.3.1		