Definition of Terms and Acronyms

a. Policy
This policy, the PICORP Berhad General IT Policies

b. IT Resources
IT Resources include but is not limited to computer networks, network servers, personal computers, workstations, voice and video networks, transmission systems, and digital information.

c. Login ID
Normally consist of username and password, used by users to login into a computer system, e-mail, or other internet based services

d. Staff
Employees of PICORP Berhad and its Subsidiaries and Associates Companies

e. PICORP Berhad
Progressive Impact Corporation Berhad and its Subsidiaries and Associate Companies

f. ASMA
Alam Sekitar Malaysia Sdn Bhd

g. ASMA EIT Department
ASMA Environmental Information Technology Department

h. Subsidiaries
Alam Sekitar Malaysia Sdn Bhd,
ALS Technichem (M) Sdn Bhd,
Alam Sekitar Eco-Technology Sdn Bhd,
Asma International Sdn Bhd,
And all other subsidiaries under PICORP Group

i. Associates Companies
Zaiyadal Keluarga Sdn Bhd Group of Companies
PITECH Group of Companies

Introduction

The objective of development of the PICORP Berhad General IT Policy is to establish a common framework for adopting and deploying IT Resources within Progressive Impact Corporation Berhad and its Subsidiaries and Associate Companies ("PICORP Berhad ").

The Policy has been established in order to:

a) Provide PICORP Berhad with a controlled and secured integrated IT environment to support the business operations' needs and to enable seamless flow of information across the organization in a timely, accurate and cost effective manner,

b) Safeguard the privacy, confidentiality and reliability of information,

c) Protect and maximize PICORP Berhad 's investment in IT Resources,

d) Reduce PICORP Berhad 's business and legal risks, and

e) Define the responsibility and the requirements on the use of IT Resources within PICORP Berhad environment.

This policy may either be implemented independently or complemented within the existing PICORP Berhad’s policy.

1.0 Purpose

a) The Policy provides guidance about acceptable use of any IT Resources, not limited to hardware, software and networks, provided by PICORP Berhad. The Policy also describes the standards of which Staff are expected to diligently observe when using these facilities, and ensures that Staff are aware of the legal consequences attached to inappropriate use of these facilities.

b) The Policy establishes a framework within which Staff of PICORP Berhad can apply self-regulation to their use of IT Resources.

c) The Policy is designed to advise Staff that their usage of PICORP Berhad's IT Resources is for official purposes only. Usage will be monitored and, in some cases, recorded. Usage of IT Resources in breach of the Policy may lead to appropriate disciplinary action being taken as described in the PICORP Berhad’s Human Resource Policy and Procedures Manual.

d) The Policy also specifies actions that PICORP Berhad will take in the investigation of complaints received from both internal and external sources on any unacceptable use of PICORP Berhad's IT Resources.

2.0 IT Facilities Policies

The main purpose for the provision of information technology facilities policies is for use in connection with training, learning, research & development and approved business activities of PICORP Berhad by its Staff and other authorized personnel. For the protection and benefit of PICORP Berhad and its Staff, any person using IT Resources must abide by the Policy set henceforth. This Policy can be accessed at http://enviromalaysia.com.my, or can be requested from ASMA EIT Department.

To ensure that IT Resources are not abused, PICORP Berhad retains the right to monitor messages and materials sent across or stored in computers or storage areas managed by PICORP Berhad and to take any appropriate action if it comes to PICORP Berhad's attention that access to IT Resources is being abused or misused.

a) IT Resources must be treated with care and used only in accordance with the proper operating instructions. Any apparent fault with IT Resources should be reported promptly to the relevant authority in PICORP Berhad. IT Resources must not be used if there is reason to believe that it may not be in safe working order or condition.

b) The use of any IT Resources for storage and/or transmission of materials, which PICORP Berhad considers to be obscene and/or offensive, are strictly prohibited. IT Resources must not be used to download pornographic, obscene, excessively violent, and/or offensive materials from the Internet.

c) Computer programs in any of the IT Resources are protected by the law of copyright. Staff shall not install or download any computer programs or any unlicensed pirated versions of computer programs irrespective of whether they are used for the benefits of PICORP Berhad or otherwise, without prior written approval from PICORP Berhad.

d) Online resources, which are owned by PICORP Berhad or subscribed to by PICORP Berhad, are protected by copyright and license agreements. Staff authorized to utilize the online resources owned by PICORP BERHAD or licensed by third party providers must abide with PICORP Berhad's or the Licensor's terms and conditions of usage at all times.

e) When any of PICORP Berhad's IT Resources are used to legally access any authorized external network and/or computer facilities related to their work or for the performance of their duties and obligations to PICORP Berhad, Staff must also abide by any additional conditions imposed by the providers of such facilities.

f) PICORP Berhad views the unauthorized access or interference with any of its IT Resources as an extremely serious disciplinary offence. Any breach of these regulations shall be dealt with in accordance with the disciplinary procedures of PICORP Berhad. In the case of a serious breach, the authorization of Staff to access and use particular IT Resources may be withdrawn immediately, pending disciplinary action being taken against the staff by PICORP Berhad's management.

3.0 Computing Ethics and Staff Responsibilities

This section delineates the responsible use of PICORP Berhad IT Resources.

IT Resources at PICORP Berhad are owned by PICORP Berhad and managed and administered by ASMA EIT Department. PICORP Berhad will provide access to appropriate central and individual computing resources, and to their attached networks to Staff whose tasks require such facilities. Staff are responsible for managing their use of IT Resources and are accountable for their actions relating to IT Resources security.

3.1 General Responsibilities

Staff must abide by the following list of standards that have been established, and promptly report any weaknesses in PICORP Berhad's computer security, any incidents of possible abuse or misuse, or violation of these policies to PICORP Berhad:

a) Access only information that is your own, that is publicly available, or to which you have been given authorized access. Staff may use only IT Resources they are authorized to use and only for the purposes specified when their accounts were issued or permission to use the resources was granted.

b) For security reasons, protect your Login ID, password, and system from unauthorized use. Staffs are advice to change the password periodically and DO NOT shares your login access with other individual.

c) DO NOT attempt to circumvent or subvert system, network, or resources of the Internet, destroy the integrity of computer-based information, or access controlled information and/or systems without formal authorization.

d) DO NOT install software/hardware for personal use on IT Resources. This includes any unlicensed or pirated software even if such software is used or intended to be used by Staff for purposes of carrying out his/her work, duties and responsibilities to PICORP Berhad.

e) Staff must not conduct activities that might interfere with the operational performance and/or integrity of PICORP Berhad's IT Resources. Examples of these activities include playing games, listening or viewing streaming audio/video for recreation, and intentionally running programs that attempt to violate the operational integrity of IT Resources.

f) Staff are prohibited from using PICORP Berhad's IT Resources for personal or commercial gain, such as, selling access to your Login ID or to IT Resources, performing work for profit with PICORP Berhad resources in a manner not authorized by PICORP Berhad, marketing/advertising, and/or personal business transactions.

g) IT Resources are not to be used for partisan political purposes, such as using electronic mail to circulate advertising for political candidates or lobbying of public officials.

h) DO NOT use electronic mail or other electronic messaging services to harass or intimidate others, for example, by broadcasting messages, or by repeatedly sending unwanted electronic mails.

i) Respect the rights of others by complying with all PICORP Berhad's policies regarding sexual, racial and other forms of harassment, and by preserving the privacy of personal data to which you have access.

j) Respect all pertinent licenses (including software licenses), copyrights, contracts, and other restricted or proprietary information. Use only legal versions of copyrighted software in compliance with vendor license requirements.

k) Respect the integrity of IT Resources, for example, by not intentionally developing programs or making use of already existing programs that harass others, or infiltrate a computer or computing system, and/or damage or alter the software components of a computer or computing system, or gain unauthorized access to other facilities accessible via the network.

l) Respect and adhere to any local, state or federal law, which may govern the use of information technology or communication networks.

m) Acknowledge that the privacy and confidentiality of electronic information transmissions cannot be guaranteed, for example, electronic mail is generally not secure and is vulnerable to unauthorized access and modification.

n) Acknowledge that authorized PICORP Berhad 's personnel may examine computing resources, communication systems, files, electronic mail, and printer listings for reasons including but not limited to troubleshooting hardware and software problems, preventing or investigating unauthorized access and system abuse or misuse, assuring compliance with software copyright and distribution policies, and complying with legal and regulatory requests for information.

o) Staff must, through their own initiatives, gain the basic knowledge in information technology, especially on issues relevant to their basic IT operational needs, including for the purpose of understanding this Policy.

p) Staff must not use the IT Resources for intentional creation, downloading, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials.

q) Staff must not use the IT Resources for intentional creation, downloading, viewing, storage, copying or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal or immoral activities/purposes or activities/purposes otherwise prohibited by PICORP Berhad's policies or the laws of Malaysia.

r) Staff must not use IT Resources for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services).

s) Staff must not use IT Resources for engaging in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

t) Staff must not use IT Resources for posting agency or personal information to external newsgroups, bulletin boards or other public forums without authority, including information which is at odds with PICORP Berhad missions or positions. This includes any use that could create the perception that the communication was made in one's official capacity as an employee of PICORP Berhad, unless appropriate approval has been obtained.

u) Staff must not use IT Resources as a staging ground or platform to gain unauthorized access to other systems.

v) Staff must not use IT Resources for creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of subject matter. These activities shall be regarded as "spam mailing" which are an abuse or misuse of IT Resources and shall not be tolerated by PICORP Berhad.

w) Staff must not use IT Resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.

x) Staff must not add, or install, his/her personal IT software or hardware to existing IT Resources without the appropriate management authorization.

y) Staff must not use IT Resources in a manner which could generate additional expenses to PICORP Berhad.

z) Staff must not use IT Resources for intentional unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes information subject to the relevant IT Act(s), copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

aa) Staff must ensure that they are not giving false impression that they are acting in an official capacity when using IT Resources for personal purposes. Any Staff which gives or provides such shall be personally liable for any liabilities caused to or suffered by PICORP Berhad arising from the misrepresentations made by Staff and the use of IT Resources for personal purposes for which such false impression was given.

bb) Staff must diligently follow policies and procedures in their use of IT Resources (e.g., Internet, e-mail, shared data, etc) and refrain from any practices, which might jeopardize IT Resources, including but not limited to virus attacks, when downloading files from the Internet.

cc) Staff must learn about Internet etiquette, customs and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.

dd) Staff must familiarize themselves with any special requirements for accessing, protecting and utilizing data, including privacy requirements, copyright requirements, and procurement of sensitive data.

ee) Staff must not by any deliberate or careless act or omission, jeopardize or seek to jeopardize the integrity of any IT Resources.

ff) Staff must not access and/or attempt to access any IT Resources which they are not properly authorized to access. In particular, the confidentiality of data belonging to other Staff must be respected.

gg) Staff must take all necessary steps to protect and maintain the confidentiality of any passwords allocated for their use. Staff must not use login credentials that belong to someone else.

hh) Staff must not use any IT Resources for a purpose other than that for which they are authorized. Staff must seek advice if they have any doubt about their authority to use any of the IT Resources.

ii) Staff must comply with all their legal obligations affecting their use of IT Resources.

jj) Staff must take all reasonable steps to exclude and avoid the spread of malicious software, programs or codes, e.g. viruses, worms, spywares, malwares, etc. and must co-operate fully with all measures instituted by PICORP Berhad to prevent the spread of such software, programs or codes. Staff must comply with any instruction provided by PICORP Berhad in relation to any such software, programs or codes if they are detected by PICORP Berhad in IT Resources. In particular, Staff must not install or execute on IT Resources any software obtained from a third party source, unless such software has been previously checked and cleared of the presence of malicious software, programs or codes by PICORP Berhad personnel or appropriate technical personnel. It is an offence to knowingly corrupt a computer program or any data stored in the computer system.

kk) Staff must comply with all their legal obligations concerning copyright, and must not copy any software or other data without the prior authorization from the copyright owner. Such action would be in breach of copyright law. Furthermore, Staff must comply with any contractual obligations imposed on PICORP Berhad concerning the use of any IT Resources by any third party.

ll) Staff must not connect any unauthorized equipment to PICORP Berhad network without consultation and prior written approval from authorized personnel. If PICORP Berhad has reasonable grounds for believing that any equipment may be the cause of unacceptable degradation of network performance detrimental to other Staff, then Staff must co-operate with the disconnection of the equipment from the network pending resolution of the problem.

mm) Staff must not make libelous or defamatory statement in any manner whatsoever when using any IT Resources. Staff shall be personally liable and shall indemnify PICORP Berhad for damages or losses suffered as a result of Staff making such statement.

nn) Health and safety with regards to computer equipment and computer work stations should be managed within the context of the general and any specific Health & Safety policies and procedures within PICORP Berhad. All Managers are responsible for ensuring the implementation of the health & safety legislation and procedures with regards to computer equipment within their respective Departments.

oo) It is the responsibility of Department Managers to ensure appropriate computer training for their staff is identified.

pp) The ASMA EIT Department maybe called upon for any advice on computer-related issues.

qq) For security and confidentiality purposes, the employee may not forward Company email to personal email accounts, such as Gmail, Hotmail, Yahoo, AOL or others. Additionally, the Employee may not forward personal external email account messages to Company email accounts. The use of non-Company email accounts for sending message in Company is prohibited.

rr) Using of personal internet mobile broadband connection is not allowed in the company.

The above lists are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use, abuse or misuse.

Staff who violates this Policy will be subjected to PICORP Berhad disciplinary processes and procedures which may include dismissal of the staff concern. Privileges to use the IT Resources may be revoked. Illegal acts may also subject Staff to prosecution by local, state, and/or federal authorities.

4.0 Guidelines For Handling Computer System Incident

Do not panic. Call the ASMA EIT Department. Its personnel will guide you through the next steps to take, which includes the following:

a) Assessment: Do not immediately shut down the computer, as you may lose important information. If the computer is being used to attack others, or if the attacker is actively using or damaging the computer, you may need to disconnect it from the network. If this does not appear to be the case, leave the computer connected for the moment.

b) System scan: Run an emergency system security scan. The security scan is done through the Safe Mode of Microsoft Windows operating system without any configuration for the network connection loaded. This will ensure that the computer will boot up without allowing any means for attack, or for any viruses to load itself.

c) Gather all relevant information: This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and database activity logs.

d) Take notes: Record all relevant information, including things you observed, actions you took, dates and times, etc. It is best to log your activities as they are done.

e) Change login password: Change all administrator, root or any other high credential login accounts residing in the computer system that was involved with the incident.

f) ASMA EIT Department personnel will determine the correct course of action: Depending on the seriousness of the incident, the next course of action may be to "clean up" and move on, or attempt to catch the individual causing the incident.

g) Engage Professional Consultant: PICORP Berhad may acquire services from professional consultant to do the analysis and system audit, and repairing the computer affected by the incident. PICORP Berhad may also perform professional audit by an independent qualified computer security incident specialist/analyst.

5.0 Virus Protection

5.1 Purpose

The purposes of this section of the Policy are:

a. To establish procedures that defines Staff responsibilities in reducing threats of computer viruses to IT Resources.

b. To establish responsibility for overseeing computer virus prevention activities in PICORP Berhad, and to establish a reporting mechanism to ensure all appropriate personnel are alerted in case of a computer virus incident.

c. To promote awareness of the threat posed by computer viruses, and to ensure that virus protection software and procedures are properly implemented and utilized on a regular basis.

d. To ensure computers used by Staff are installed with anti-virus program. Staff have to make sure the anti-virus program is not disabled, bypassed, or modified in any way to render it un-reliable. This is to eliminate any possibility of a network-wide virus infection or disruption of productivity.

5.2 Specific Restrictions

PICORP Berhad expressly prohibits:

a. Development of any form of computer virus with the intent to distribute through PICORP Berhad 's network or beyond.

b. Intentional distribution of a virus, regardless of type (nuisance or destructive).

c. Intentional creation of false alarms using hoax messages.

5.3 Staff Responsibilities and Preventive Measures

Malicious software covers all software which has been deliberately designed to harm computer systems. Such software spreads from one system to another through email (normally attachments) exchange or download of files from infected floppy disks or embedded into computer games. The computer systems that have anti-virus installed, and anti-virus definition files updated periodically, may be sufficiently protected. However, you should be aware that the anti-virus software cannot automatically detect newly developed viruses. Staff should therefore take the following responsibilities and precautions to guard against virus or other type of malicious attacks:

a) Understand the risks associated with viruses and preventive measures that can be taken,

b) Be aware of and follow the procedures outlined in ASMA EIT Department announcements as distributed via emails, which will be used to alert Staff of potential computer virus threats, and to take appropriate recommended preventive actions.

c) Treat nuisance viruses with the same urgency as destructive viruses. Write down the name of the virus, if provided by the virus detection software.

d) Write down any recent unusual computer activities (for instance, unexpected disk access, error messages, or screen displays) and, if possible, the date and time of the first noticeable occurrence.

e) Contact ASMA EIT Department personnel when a computer virus is suspected and/or detected.

f) Staff must become familiar with the operation of the anti-virus software and must follow the procedures recommended by ASMA EIT Department in operating such software.

g) Staff must ensure that the anti-virus system installed in the computer is operating properly.

h) Staff must configure the anti-virus software so that it automatically scans incoming documents whether via e-mail, internet or via PICORP Berhad internal network computers and servers.

i) Contact ASMA EIT Department personnel if the automatic anti-virus update subscription for the anti-virus program has expired and does not updated automatically.

j) Never boot directly from a floppy diskette unless the diskette has been scanned for viruses. Staff must ensure the antivirus program is configured to automatically scan all floppy disks upon use.

k) Staff must not open email attachments from unsolicited or un-trusted sources.

l) Ensure files received from external sources are free of viruses prior to use or distribution.

m) Contact ASMA EIT Department personnel if the automatic anti-virus update subscription for the anti-virus program has expired and does not updated automatically.

n) Never boot directly from a floppy diskette unless the diskette has been scanned for viruses. Staff must ensure the antivirus program is configured to automatically scan all floppy disks upon use.

o) Contact ASMA EIT Department personnel if the automatic anti-virus update subscription for the anti-virus program has expired and does not updated automatically.

p) Never boot directly from a floppy diskette unless the diskette has been scanned for viruses. Staff must ensure the antivirus program is configured to automatically scan all floppy disks upon use.

q) Staff must not open email attachments from unsolicited or un-trusted sources.

r) Ensure files received from external sources are free of viruses prior to use or distribution.

s) Staff must not use unsolicited floppy disks or CD-ROMS received from un-trusted sources.

t) Never use or introduce non-licensed software, unsecured or unverified files and software on IT Resources.

u) Back up important and business critical data to a drive on the server (see ASMA EIT personnel for access requirements) at least once a week or more often for highly critical data.

6.0 Back Up

a) The ASMA EIT Department is responsible for ensuring the implementation of an effective back-up strategy for server-held software and data.

b) Users of networked desktop PCs should avoid storing important data on their local hard drives. Data stored in this manner may be lost if a problem develops with the PC, and the ASMA EIT Department may not be able to assist in its recovery. Data should be stored within the file directory (folder) structure used by the office.

c) Remote and laptop/notebook PC users must ensure they back up their data regularly. The ASMA EIT Department will provide advice and assistance.

d) Staff must not store their personal file not related to PICORP Berhad business in the file directory (folder) structure used by the office (in the server).

7.0 Mobile Devices

Mobile devices, such as PDA, notebook, pen-drive, etc., are not considered as secure computing devices. It is recommended that only non-confidential information be stored on these devices and further protected by enabling the password protection feature.

In cases where there is a justifiable business need or requirement for confidential information, such as business strategy information, confidential operational information, employee information, etc., to be stored or transferred to these devices, appropriate security measures must be implemented as listed below:

a) Removable media such as memory cards must not be used to store confidential information.

b) These devices must be password protected using the security feature provided on the devices and there should be no sharing of the passwords.

c) A Desktop PC that is used for synchronization with the mobile devices must have approved anti-virus software installed.

d) Confidential information shall not be stored, downloaded, or leave PICORP Berhad premises unless justified and approved by Staff superior.

e) Confidential information shall not be shared with others who do not have a job-related need for the information. Any sharing of confidential information must be on a strict job-related "need to know" basis. If Staff suspects that any confidential information in his/her care has been leaked or is made known to others without Staff knowledge and approval, Staff must immediately inform ASMA EIT Department personnel. The ASMA EIT Department personnel shall conduct checks on the IT Resources used by Staff.

f) Confidential information must be encrypted and protected to the best of Staff capabilities.

g) Whenever there is no longer the need to access or store this confidential information, it must be deleted from the mobile devices.

8.0 Copyright and Computer Software

Copying, adapting, and/or electronically transmitting computer software is strictly forbidden except:

a) where a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with IT Resources and that it is used in no other manner,

b) where a new copy and adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful,

c) where appropriate, written consent (from the holder of such copyright) is obtained,

d) where the software is in the public domain, and appropriate documentation can be provided.

Computer programs may not be rented, leased, or loaned for direct or indirect commercial purposes. Lawful transfer of possession of a legally licensed computer program may be exempted, provided there are no existing copies left on the original computer.

PICORP Berhad prohibits the unauthorized copying or electronic transmission of computer software, data, and software manuals, unless appropriate written consent is obtained from the vendor and/or copyright holder.

9.0 Use of Electronic Communications

PICORP Berhad and its employees recognize that a substantial portion of any information (including email and other communications and records of account usage) that is stored in IT Resources is accessible as such to any person at any time. PICORP Berhad shall not, in an arbitrary manner, selectively record or monitor the information transmitted or stored by its employees. Nothing in this undertaking shall:

a) constitute PICORP Berhad as the guarantor of the privacy or security of any such information,

b) prohibit PICORP Berhad from having access to such information in order, in accordance with its acceptable use Policy, to:

   i. back up and maintain the functionality of its electronic communications systems,

   ii. enforce any lawful prohibition against the use of such systems for personal or commercial purposes,

   iii. prevent or investigate unauthorized access to such systems,

   iv. enforce any requirements of law, and

   v. enforce any software or other licensing agreements or copyrights.

c) prohibit PICORP Berhad from having access to such information in order to comply with a subpoena lawfully issued, to comply with a request for public records under the relevant act, or to comply with any similar order or requirement of law,

d) prohibit PICORP Berhad from installing "spam" filters, firewalls, virus detectors or any software or equipment that limits the use of or access to its electronic communications systems,

e) prohibit PICORP Berhad from monitoring and logging usage data on a routine basis, including network session connection times and end points, CPU and disk utilization for individual Staff, security audit trails, and network loading, pursuant to an acceptable use policy or as in incident of the troubleshooting, repair or maintenance of its electronic communications systems or the preservation or enhancement of their functionality,

f) prohibit any person who is the lawful recipient of any electronic transmission or communication from making such disclosure of it as he or she chooses, or permit any employee to alter any PICORP Berhad's electronic communications system (by altering, adding or deleting any software or equipment) or any PICORP Berhad's website or its associated links without PICORP Berhad's prior written approval.

10.0 Legal Consequences for Abuse or Misuse of PICORP Berhad's IT Resources

In cases involving civil or criminal law, electronic data (deleted or otherwise) can be produced as evidence in hard copy. There are a number of areas of law and regulations which apply to the use of electronic data and which could involve liability of Staff of PICORP Berhad. These include the following:

a) Intellectual property: Anyone who uses email to send or receive any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorized by them.

b) Obscenity: A criminal offence is committed if a person publishes any material which is pornographic, excessively violent of nature or which comes under the provisions of the respective Act(s).

c) Defamation: As a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people, or an organization. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or entity will rest mainly with the sender of the email.

d) Data Protection: Processing information (including photographs) which contains personal data about individuals requires the express written consent of those individuals.

e) Discrimination: Any material disseminated which is discriminatory or encourages discrimination may be unlawful under the respective Act(s), where it involves discrimination on the grounds of sex, race or disability.

f) Contravention: Contravention of the PICORP Berhad IT Policy or any act of deliberate sabotage to PICORP Berhad computer systems may be considered a disciplinary offence.

11.0 Disciplinary Process

Access to PICORP Berhad information technology resources is a privilege subjected to appropriate use. Violation of the Policy will be reported to the appropriate authority and Human Resource Department.

The ASMA EIT Department personnel shall investigate and review all complaints or instances of unacceptable use brought to their attention. Suspected or known abuse or misuse of IT Resources may, pending the result of a thorough investigation, result in disciplinary actions being taken against the offender. The severity of the disciplinary action shall be in accordance to guidelines and procedures set forth in PICORP Berhad's policies, codes, regulations or laws enforced from time to time. Please refer to the latest available policies.

In addition to the Policy, all existing statutory laws, regulations, codes and relevant policies implemented by PICORP Berhad, not limited to those specifically applicable to IT Resources, shall be applicable as well.

12.0 Amendments to This Policy

PICORP Berhad reserves the right to amend this policy at any time. Staff will receive notification of all such amendments prior to their effective date.

SUBJECT: IT POLICY

I, _____ hereby acknowledge that I have read and understood the IT Policy.

Signature of Employee: _____

Date: _____

Signature of Witness: _____

Date: _____