



Communications and Multimedia
Consumer Forum of Malaysia

1st June 2005

**Internet Access Service Provider (IASP) Sub-Code for
the Communications and Multimedia Industry
Malaysia**



Communications and Multimedia
Consumer Forum of Malaysia

TABLE OF CONTENTS

PART 1 - INTRODUCTION	2
PART 2- GENERAL RULES OF THE CODE FOR INTERNET ACCESS SERVICE PROVIDERS	6
PART 3- REVIEW AND AMENDMENTS	14

1. Background

1.1 The Communications and Multimedia Act 1998 (CMA 1998) seeks to establish a regime of industry self-regulation, supported by fallback regulatory standards that may be administered by the Malaysian Communications and Multimedia Commission (MCMC).

1.2 Pursuant to section 189 of CMA 1998, MCMC had designated the Communications and Multimedia Consumer Forum of Malaysia (Consumer Forum) as the consumer forum in March 2001. The Consumer Forum has been given the responsibility to develop sub-codes for dealing with matters relating to the protection and promotion of consumer interests in relation to specific services including, but not limited to, the matters listed in the CMA 1998.

(a) The Consumer Forum has identified the Internet Access Service Provider Sub-Code (hereinafter referred to as the "IASP Code") as being one of the important sub-codes for the Consumer Forum to be developed at this juncture.

(b) A permanent working committee appointed pursuant to Article 19 of the Constitution of Forum Pengguna Komunikasi dan Multimedia Malaysia made up of relevant parties from both the demand and supply side of the communications and multimedia services drafted the following IASP Code.

2. Preamble

2.1 This IASP Code is cognizant of the constant state of profound technological change that is characteristic of the communications and multimedia industry.

- 2.2 As technologies innovate new operating conditions, this IASP Code may need to be updated to nurture, conserve and protect the objectives of this IASP Code.

Objectives of the Code

- 3.1 To promote the free-flow of information and communications over the Internet;
- 3.2 To set out a code of practice for Internet Access Service Providers.
- 3.3 To improve the standard of conduct within the industry.

4. Definitions

- 4.1 All capitalised terms in this IASP Code shall bear the same definition as contained in the General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia (GCC) unless specifically otherwise provided herein.

- 4.2 For the purpose of this Code:

“Acceptable Use Policy” or “AUP” means a policy defined by the Service Provider as to the acceptable nature of use of a service subscribed.

“Child” means all persons under the age of 18 years as defined by the Child Act 2001.

“Code” means this IASP Code.

“Consumer Forum” means the Consumer Forum of Malaysia set up pursuant to the CMA 1998.

“CMA 1998” means the Communications and Multimedia Act 1998 including any amendments thereto from time to time.

“Consumer” means a person who receives, acquires, uses or subscribes to the Internet access service provided by any Service Provider. This includes a Customer.

“Customer” means a person who, for consideration, acquires or subscribes to the Internet access service provided by any Service Provider.

“GCC” means General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia.

“Guardian” means natural parent or any person having care and control over a child.

“Internet” means a global information system that is able to support communications using the Internet Protocol (IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols.

“Internet Access Service” means an applications service whereby a person is able to access Internet services and applications.

“Internet Access Service Provider” or **“IASP”** means a person who provides Internet Access Service.

“MCMC” means the Malaysian Communications and Multimedia Commission established under the Malaysian Communications and Multimedia Commission Act 1998.

“Personal Information” means any information collected by the Service Provider from the Customer that identifies the Customer.

“Service Provider” means the service provider as set out in Section 5.1 (Part 1).

“Spam” means unsolicited electronic messages sent through various communication modes including but not limited to e-mails, mobiles short message (SMS) or instant messaging services where there is no prior relationship between the sender and the recipient regardless of content whether commercial or non-commercial messages including malicious program and/or data.

“Website” means a file that contains text, audio and/or visual data accessible on the World Wide Web by a single Uniform Resource Locator (URL).

“World Wide Web” means the network of websites accessible on the Internet using including, but not limited to, the Hypertext Transfer Protocol (‘http’).

5. Scope

5.1 This Code shall be applicable to the following:-

- (a) IASPs;
- (b) Other persons or class of persons as may be directed by MCMC; and
- (c) Members of the Consumer Forum.

(For the purposes of this IASP Code, the code subjects shall be referred to as “Service Providers”.)

5.2 This IASP Code may be amended from time to time.

5.3 This IASP Code is developed pursuant to Clause 6.2, Part 1 of the GCC to address the specific needs of the Internet services industry.

5.4 This IASP Code is to be read in addition to and not in derogation of the GCC. The GCC will govern all sub-codes unless expressly otherwise provided in the sub-codes.

5.5 This IASP Code shall come into effect upon registration in accordance with the CMA 1998. However, Service Providers shall be granted a grace period of six (6) months, or such period as may be extended by the Council of the Consumer Forum to comply with the provisions of this IASP Code.

The IASP Code general rules are as follows:-

1. The IASP Code Guiding Principles
2. Protection of Personal Information
3. Provision of Information
4. Provisioning of Services
5. Anti-Spam Measures
6. Policy on Information Network Security
7. Content
8. Billing
9. Protection of Minor
10. Handling of Customer Complaints and Disputes

Principle of Compensation

1. The IASP Code Guiding Principles

1.1 The communications and multimedia industry will strive to achieve the following principles:

- (a) The National Policy Objectives as set out in the CMA 1998;
- (b) The Code objectives as set out in Clause 5, Part 1 of the GCC;
and
- (c) The Fundamental Principles for Service Providers as outlined Clause 1(A), Part 2 of the GCC for the communications and multimedia industry of Malaysia.

2. Protection of Personal Information

2.1 The relevant provisions in the GCC on protection of consumer information (namely the provisions of Clause 2, Part 2 of the GCC) are applicable to the IASP Code.

3. Provision of Information

3.1 Service Providers shall comply with all the relevant provisions contained in the GCC on the provision of information regarding services, rates and performance.

3.2 Consumers shall be provided with adequate description of the service offered prior to entering into the contract of sale. All material features of the services such as bandwidth, speed and availability (i.e. coverage) should be described in simple language that is easily understood.

3.3 The IASP Code should impose an obligation on all Service Providers to publish and adhere to an acceptable use policy, which in all cases would be a condition of sale. This policy shall, at the minimum, include:

(a) Information to Consumers about their legal obligations and liabilities in making use of the services provided by the Service Provider;

(b) Information to Consumers about the responsibilities of the Service Providers in ensuring that the Customers adhere to their legal obligations;

(c) Information on Internet use etiquette;

(d) A description of practice, which are abusive and therefore prohibited; and

(e) Subject to the anti-spam measures herein provided, an indication of the type of remedial measures that may be taken by the Service Providers in respect of defaulting Customers.

3.4 Service Providers shall take reasonable steps to notify all Consumers of their policy on privacy prior to the entering into the contract of sale.

3.5 Any changes in policies developed by the Service Providers should also be communicated to the Consumers as soon as practicable.

4. Provisioning of Services

4.1 Service Providers will provide services and products in a responsible manner, ensuring that the services that they provide to their Customers meet the service levels as contractually agreed between the Service Providers and the Customers.

4.2 Service Providers shall endeavour to provide consistent and reliable access to the services.

4.3 Service Providers shall give adequate notice to their Customers of any planned interruptions of service.

4.4 Service Providers shall not discriminate unduly between persons or classes of persons in the provision of their services or any related matters and shall provide equal access to all Customers.

5. Anti-Spam Measures

5.1 The Service Providers should address concerns about Spam and consider methods of managing such issues in such a way to ensure the protection of the Customers' interest. The Service Provider may consider the following measures in dealing with these issues: -

(a) To articulate a specific definition for Spam so as to be clear what is being addressed.

(b) To include the following general principles as contractual conditions in agreements entered into between the Service Providers and Customers who may have the propensity to produce Spam:-

(i) The Customer shall not engage in sending Spam messages;

(ii) Any breach of conditions shall result in the suspension and/or termination of the Customer account. Such Customer may appeal for reactivation of the said account in accordance with the Service Provider's prevailing policies and procedures;

(iii) Service Providers should provide specific guidance (in the form of an Acceptable Use Policy (AUP)) on when sanctions or suspension and termination of account would be imposed. The Acceptable Use Policy should impose an obligation on the Customer to ensure that all commercial e-mails sent out by the Customer are accompanied by or include the following information:-

(a) Header information that is not false, deceptive or misleading

(b) A valid return e-mail address

(c) Functional unsubscribe facility (ie "opt out" facility)

(d) Identity of sender

(e) Message be clearly labeled as commercial communication (eg [ADVERTISEMENT] for advertisements, [COMMERCIALS] for commercials etc.)

For the purpose of this provision, "commercial electronic message" shall mean any electronic message that can be concluded to be for the purpose of advertising, highlighting, promoting, selling and/or offering to supply any goods, property, service and/or business or investment opportunity.

(iv)The Service Providers should also provide their policies and procedures in reactivating the services suspended due to violation of the AUP.

5.2 In addition to the terms and conditions outlined above in the service contract with their Customers, Service Providers should also consider implementing some technical measures to assist in curbing Spam.

5.3 In addition to Section 5.1(b)(iv), the Service Providers shall have a written procedure for handling incidents of Spam. This procedure should be publicly available either in print and/or on a web site. Examples of such procedure may be as follows:-

- (a) There shall be an 'abuse' account. Mail sent to this account shall be routed to a responsible person or those who have the ability to investigate and take action on such complaints;
- (b) All complaints sent to the 'abuse' account shall be replied to. All complaints should be investigated within certain period of time and proper and timely replies should be given to complainants
- (c) Complaints shall be investigated and action must be taken against users flouting the terms and conditions referring to Spam. Even if investigation reveals no fault on the part of the Service Provider or

user, the Service Provider is encouraged to help the complainant to resolve their complaint.

- 5.4 The Service Provider shall make available on its website information on anti-spamming measures regarding its Customers. Such information may include IP addresses suspended and/or blocked by the Service Provider and/or any anti-spamming monitoring bodies such as Spamhaus and Spamcop. The said information shall be updated on a weekly basis.

6. Policy on Information Network Security

6.1 Service Providers should have a guideline on how to implement security in their network and there must be some level of standard procedures to be followed. The policy may cover the following areas:-

(a) Business Continuity Planning

There must be a business continuity plan in place to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

(b) System Access Control

Access Control System should be in place to ensure the following:-

- (i) to control access to information
- (ii) to prevent unauthorised access to information systems
- (iii) to ensure the protection of networked services
- (iv) to prevent unauthorized computer access
- (v) to detect unauthorised activities.

(c) System Development and Maintenance

Service Providers should also put in place policies on system development and maintenance so as to ensure the following:-

- (i) security is built into operational systems;

- (ii) to prevent loss, modification or misuse of user data in application systems;
- (iii) to protect the confidentiality, authenticity and integrity of information;
- (iv) to ensure IT projects and support activities are conducted in a secure manner;
- (v) to maintain the security of application system software and data.

(d) Physical and Environmental Security

Policies must be put in place to prevent: -

- (i) unauthorised access;
- (ii) damage and interference to business premises and information;
- (iii) loss, damage or compromise of assets and interruption to business activities; and
- (iv) compromise or theft of information and information processing facilities.

(e) Compliance

The policies in place must clearly set the following:-

- (i) to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
- (ii) to ensure compliance of systems with organizational security policies and standards
- (iii) to maximize the effectiveness of and to minimize interference to/from the system audit process.

(f) Security Organisation

The policies in place must clearly set the following:

- (i) to manage information security within the Company;
- (ii) to maintain the security of organizational information processing facilities and information assets accessed by third parties
- (iii) to maintain the security of information when the responsibility for information processing has been outsourced to another organization.

(g) Computer & Network Management

The policies in place must clearly set the following:

- (i) to ensure the correct and secure operation of information processing facilities;
- (ii) to minimise the risk of systems failures;
- (iii) to protect the integrity of software and information;
- (iv) to maintain the integrity and availability of information processing and communication;
- (v) to ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- (vi) to prevent damage to assets and interruptions to business activities;
- (vii) to prevent loss, modification or misuse of information exchanged between organizations.

(h) Asset Classification and Control

To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

6.2 Service Providers are required to ensure that their policy on information and network security is in compliance with and subject to other general guidelines such as frameworks and determinations issued as well as framework and determinations to be issued by MCMC and Ministry of Energy, Water and Communications from time to time.

7. Content

Reference should be made to the relevant provisions of the Content Code in this regard.

8. Billing

Reference should be made to the relevant provisions of the GCC in this regard.

9. Protection of Minor

9.1 Service Providers will take reasonable steps to ensure that post- paid Internet access accounts are not provided to any child without the consent a Guardian. For the avoidance of doubt this obligation shall not be applicable to the pre-paid Internet access services.

9.2 Service Providers should take reasonable steps to provide Customers with:-

(a) information on supervising and controlling a child's access to Internet content;

(b) procedures which Guardians can implement to control a child's access to Internet content, including the availability, use and appropriate application of Internet content filtering software.

(c) notifying the Consumers : **“if you are below 18 years of age – prior consent of a guardian is required before you are allowed to subscribe to a post -paid Internet access account”** prior to the sale of the service.

10. Handling of Customer Complaints and Disputes

Reference should be made to the relevant provisions in the GCC in this regard.

11. Principle of Compensation

Reference should be made to the relevant provisions of the GCC in this regard.

1. Review and Amendments

1.1 A review of this IASP Code shall be conducted by the Consumer Forum:

- (a) Within 12 months from the date of implementation of this IASP Code; and/ or
- (b) As and when the Consumer Forum deems it necessary. (In line with the stipulated review at least every three years as stated in Clause 4.1 of the GCC).

1.2 Any amendments to this IASP Code shall go through the process of public consultation for a minimum of 45 days. The Consumer Forum will inform the MCMC of any amendments made to this IASP Code. Any amendments to the IASP Code shall only be effective upon registration by MCMC.