SOUTH AFRICAN INTERNET INDUSTRY CYBER SECURITY CODE OF PRACTICE

INTERNET SERVICE PROVIDERS'
VOLUNTARY CODE OF PRACTICE

FOR INDUSTRY SELF-REGULATION
IN THE AREA OF CYBER SECURITY

Version 1.1
October 2021

TABLE OF CONTENTS

PART A – PRELIMINARY

1. Preamble

1.1 ISPA recognises the enormous benefits that the Internet can bring to all South Africans, including the provision of and access to health and education services, enhanced opportunities for business and as a communications, information and educational tool.

1.2 This Code has been adopted and informed by the Internet Industry Association, Australia (IIA) and forms part of the cyber security global initiative.

1.3 The Code recognises that both Internet Service Providers (ISPs) and consumers, amongst others, can and must share responsibility for minimising the risks inherent in using the Internet.

1.4 There are measures that ISPs can take to address cyber security issues, which is why the industry has developed this Code. This Code is designed to provide a consistent approach for South African ISPs to help inform, educate and protect their customers in relation to cyber security risks.

1.5 This Code does not purport to cover all aspects of online security, but rather it is intended to coexist with measures occurring elsewhere, for example other industry initiatives and relevant national policy legislation.

1.6 While present security technologies have various levels of sophistication, ISPA remains committed to monitoring developments in such technologies and to keeping its members informed of these developments.

1.7 Through following the Code, ISPs will contribute to reducing the number of compromised computers in South Africa and thereby contribute to the overall security of the South African and international Internet.

1.8 Implementation of the measures contained in this Code will also benefit individual ISPs by offering the potential to:

1.8.1 Offer customers a greater level of confidence in the security of their Internet connections (as a potential 'service differentiator').

1.8.2 Reduce service calls from customers related to security issues; and

1.8.3 Improve awareness of suspicious activity on their networks, leading to a more timely and effective response to threats;

1.9 This Code will be subject to relevant South African legislation including the following:

(a) Consumer Protection Act 68 of 2008

(b) Electronic Communications and Transactions Act 25 of 2002

(c) Electronic Communications Act36 of 2005

(d) Films and Publications Act 65 of 1996

(e) Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

(f) Protection of Personal Information Act 4 of 2013 (POPIA)

2. Terminology and interpretation

2.1 In this Code, the following terms have the meaning shown:

Bot A single compromised computer (sometimes called a zombie).

Botnet A network of compromised computers (sometimes called a zombie army).

Firewall Protects a computer network from unauthorised access. Firewalls may be hardware devices, software programs or a combination of the two. Firewalls guard an internal computer network against malicious access from the outside and may also be configured to limit access to the outside from internal users.

Ingress / Egress address validation

Means not accepting any packets from computers that have source addresses not assigned within the ISP's allocation block. BCP 38 is the standard best practice for ingress/egress filtering to stop spoofing.

Malware Is short for malicious software and is designed to specifically damage or disrupt systems (for example a virus).

Spam Direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail sent to a data subject (as defined in the POPIA) without the consent of the data subject or by a person that is not a responsible party (as defined in the POPIA).

Virus Malicious software which attaches itself to a program or file. A computer virus can be spread by users sharing infected files or sending emails with viruses as attachments.

Worm Is similar to a virus but can spread without the need for any human action.

Zombie See Bot.

2.2 Where documents are referred to in the Code by means of URLs, the URLs are intended for reference only and the operation of the Code will not be affected where the document referred to is subsequently relocated to another URL.

3. Objectives

3.1 The aims of the Code include:

(a) Instilling a culture of cyber security within South African ISPs and their customers.

(b) Providing consistent messaging and plain language information to customers that will:
i. Raise awareness and educate them about cyber security risks.
ii. Set out simple steps that they can take to better protect themselves online.
iii Assist those whose computer has been identified as possibly compromised by providing them with steps they should take to rectify the situation.

(c) Assisting those customers who experience repeated compromises to their computers and develop a strategy to minimise the effect of such compromises to other customers on the ISP's network as well as customers on other ISPs' networks.

(d) Encouraging ISPs to identify compromised computers on their networks by:

i. Actively managing their networks; and
ii. Obtaining information on compromised computers via other trusted third-party sources.

(e) Developing mechanisms for ISPs to share information and collaborate about cyber security compromises and developments affecting other South African ISPs.
(f) Encouraging ISPs to identify and report any cyber security issue that may affect South Africa's critical infrastructure or that may have a national security dimension.

(g) Implementing these measures in a manner that protects the privacy of customers, consistent with relevant constitutional, legislative and common law obligations.

3.2 The Code provides guidance on how ISPs can:
(a) Undertake network management practices to help identify abnormal traffic patterns from an IP address or username that may indicate that a customer's computer has been compromised (see Schedule 2);
(b) Take steps to respond to any source of information that may relate to malicious activity (see sections 6.2 and 6.4);
(c) Inform a customer that their computer may be compromised (see paragraph 6.2 (a);
(d) Educate customers on what actions they can take to protect their computers from malicious activity (see section 6.3); and
(e) Notify, on a without prejudice basis, the South African authorities of a malicious activity (See Schedule 3).

The Code provides a list of resources that ISPs could access to gain intelligence on sources of attack (see Schedule 2).

4. Scope of this Code

4.1 This Code is voluntary.

4.2 This Code is applicable to ISPs who have subscribed to the Code and met the minimum standards for compliance.

4.3 The cyber security measures listed in this Code are not exhaustive, or exclusive. It is envisaged that these measures will change over time, in response to the changes in the nature of malicious activity.

4.4 The Code makes provision for the use of a Trustmark to signify to users that their ISP complies with this Code.

5. Principles

5.1 In seeking to achieve its objectives, the Code applies the following principles:

(a) Education of customers is a key element of the strategy;

(b) As far as practicable, there should be "electronic equivalence" (that is, behaviour and transactions that can take place in the real world should be permissible over the Internet without additional requirements or restrictions);

(c) The Code should be technology neutral (that is, it is applicable across networks and systems and not linked to specific proprietary technologies);

(d) The requirements of this Code should be fair to all concerned;

(e) The measures recommended in the Code should not adversely affect the commercial viability of the parties and the services they make available;

(f) There is a shared responsibility for Internet security; end users must accept some responsibility for securing access to their home computers and Internet connections (for example, by installing and keeping up to date anti-virus software, securing their wireless networks, etc.);

(g) The Code is designed to be flexible and allow for a range of responses according to ISPs' circumstances;

(h) The development of the Code is predicated on a recognition that compromised computers represent a threat to the integrity of networks;

(i) The privacy of customers is paramount;

(j) The Code draws upon existing industry best practices;

(k) It is recognised that some threats are more severe than others and ISPs should make provision for prioritisation or de-prioritisation, as the case may be, of action depending on the nature of the threat; and

(l) In some cases, ISPs may be required to report instances of compromises, malicious activity or attacks to relevant law enforcement and other government agencies or to provide reasonable assistance as required under the relevant legislation.

6. Education, detection, action, reporting

In order to comply with this Code, ISPs should undertake at least one of the items noted under each of the headings within this part of the Code – Education, Detection, Action and Reporting – except where otherwise specified in Part B. It is recognised that each ISP will implement cyber security programs that accord with its infrastructure, network and systems abilities; its position as a retail or wholesale ISP and its resources, policies and customer base.

6.1 **Educating customers**

(a) It is recommended that each new customer be provided with information, or links to information, which provides them with simple steps they can take to better protect themselves online. ISPs can comply by providing such information to their customers (e.g., on their website) and/or by providing links to such information on the iCode security pages at www.icode.org.za.

(b) An example of the information referred to in clause 6.1(a) is included in Schedule 1.

(c) Customers should be made aware of the fact that in certain circumstances, action will be taken to deal with compromised computers without prior notification.

(d) ISPs may choose the appropriate method by which to inform their customers. This could be, for example, via their website (including via the page referred to in 6.1(a) above); via a bill; by email or newsletter; or by specifying the details as part of the process by which the security incident is being managed by the ISP.

6.2 **Detection of compromised computers and other malicious activity**

ISPs can find out about malicious activity and compromised computers in the following ways:

(a) By undertaking network management practices to help identify abnormal traffic patterns from an IP address or username that may indicate that a customer's computer has been compromised; and

(b) By notification by trusted third party sources. (A list of sources is included in Schedule 2 of this Code).

6.3 **Actions to be taken in respect of compromised computers**

Where an ISP becomes aware of a compromised computer on its network, it is recommended that the ISP take action to address the problem for the protection of its customers and network integrity.

Subject to their terms of service, actions that ISPs can take when they become aware of a compromised computer include:

(a) Contacting the customer directly (by phone, email or SMS or other means);

(b) Regenerating the customer's account password to prompt customers to call the helpdesk so they can be directed to resources to assist;

(c) Applying an 'abuse' plan whereby the customer's Internet service is speed throttled;

(d) Temporarily quarantining the customer's service, for example by holding them within a 'walled garden' with links to relevant resources that will assist them until they are able to restore the security of their machine;

(e) In the case of spam sources, applying restrictions to outbound email (simple mail transfer protocol –SMTP); and/or

(f) Such other measures as determined by the ISP are consistent with their terms of service.

ISPs may choose to take one or more of the above actions, and may choose different options depending on whether it is the first time a customer's IP address or username has appeared on the source lists or whether they continue to appear on the lists and have taken no remedial action.

If the customer is unable to address the problem through the above actions, then the ISP should direct them to further information or technical support, which may be at the cost of the customer and may require the customer to seek assistance from a third-party organisation.

6.4 **Reporting of malicious activity**

(a) Where the ISP believes that the nature and extent of suspicious or malicious activity against its network may constitute a significant cyber security incident, the ISP should report the matter to the relevant government agencies as set out in Schedule 3 of this Code.

(b) In general terms, suspicious or malicious activity that could be reported to government agencies, includes, but is not limited to, activity that:

i. Is novel or not previously seen by the ISP; or
ii. Impacts well beyond the capacity of private enterprise to manage; or
iii. Involves serious malicious intent;
iv. Involves serious threats to South African telecommunications networks or other critical infrastructure; and/or
v. Has a notification requirement in terms of legislation.

7. Information sharing

7.1 It is recommended that ISPs actively share cyber security information with each other.

7.2 ISPA will actively share information regarding the operation of the Code in South Africa with the global iCode initiative and with other countries that have adopted a framework equivalent to this Code.

8. Terms and Conditions of service

8.1 It is recommended that ISPs take steps to review their terms and conditions to cover their adoption of the iCode. The scope of the review will be determined by the actions undertaken by each ISP as set out in this Part B. Where, for example, an ISP provides only educational information about online safety, it may wish to disclaim liability for reliance on such information. Where the ISP also undertakes action in respect of compromised computers, such as throttling or temporary quarantining, then it should set out the steps which it may take and the circumstances under which this will be done in its terms and conditions and disclaim liability for any damages which may arise from such action.

8.2 At the least ISPs should ensure that they have appropriate indemnities and limitation of liability clauses which protect them against the potential consequences of actions which they undertake under the iCode.

PART C – IMPLEMENTATION

9. Implementation date

9.1 This Code came into effect on 1 April 2013.

10. Compliance and Trustmark

10.1 In order to comply with this Code, ISPs need to follow the recommended minimum standard as set out in Part B. Such ISPs are obliged to use the iCode Trustmark on their websites and other communications materials subject to such terms and conditions as ISPA shall determine from time to time and any applicable intellectual property obligations.

10.2 To comply with the Code, ISPs must periodically (timeframes to be determined by ISPA) submit to ISPA or publish on their own website details of the actions they have taken to demonstrate their compliance with the Code.

10.3 The terms and conditions associated with the Trustmark may make provision for the revocation of permission to use or continue to use the Trustmark in circumstances where ISPA has reason to believe that the ISP is not complying with the Code or has not taken steps to rectify any non-compliance once notified of this by ISPA.

10.4 The Trustmark must point to the requisite information as set out in Schedule 1 of this Code. Alternatively, the Trustmark must link to a URL provided on the South African iCode website, which contains equivalent information for customers. This page may also link to additional tools and resources as ISPA may determine appropriate.

10.5 Example of Trustmark:

icode
compliant

11. Code review

11.1 This Code will be formally reviewed within 18 months from the date of implementation.

11.2 In reviewing this Code and in considering any proposed changes to it, ISPA will consult with ISPs who have participated in the pilot iCode project, appropriate government agencies and other relevant stakeholders.

The information below is to be made available by the ISP to its customer

1. Internet security is an ongoing challenge – but it is a challenge that must be met if you are to enjoy a safer and more secure online experience. As Internet users, we are all required to play our part in promoting and practising a "culture of cyber security".

2. The South African iCode recommends that the following steps be taken to help ensure that your computer stays adequately protected for a safer and more secure online experience:

   (a) **Stop and think before you click on links or attachments**. Don't open or respond to suspicious emails or attachments from unknown sources. Don't click on links in emails requesting your personal details.

   (b) **Take action immediately if you suspect your computer has been compromised.** Change your passwords immediately and contact your bank if you suspect personal financial information has been stolen.

   (c) Keep your anti-virus and other security software updated.
   (d) Install a firewall to prevent unauthorised access to your computer.
   (e) Turn on automatic updates so that all your software receives the latest fixes.

   (f) Get a stronger password and change it regularly.

   (g) **Check your "sent items" file or "outgoing" email.** If you find unknown messages in your outbox, it is a sign that your computer may be infected with spyware, and may be part of a botnet.

   (h) Stop and think before you share any personal or financial information about yourself, your friends or family online.

   (i) **Configure your wireless network securely.** If you are using a wireless router/modem, enable the security features with a strong password. Use WPA or WPA2 encryption on your Wi-Fi equipment (WEP is an older standard and is less secure). Refer to your router/modem manual or contact your ISP for further details.

   (j) Use the most recent Operating System whenever possible.
   (k) Know what your children are doing online. Make sure they know how to stay safe and encourage them to report anything suspicious. For further information about online safety go to the following sites:

   https://ispa.org.za/safety/
   https://www.fpb.org.za/
   https://www.fpb.org.za/child-protection/

3. **More Information and tools for ongoing security**

   3.1 Learn more about securing your computer at www.icode.org.za. This site offers practical tips from the Internet industry to help guard against Internet fraud, computer security, and the protection of personal information. This site also provides information about recommended products and services to help ensure ongoing protection.

   3.2 In addition, visit the following site:

   https://safety.google/security/

1. **ISP network management activities**

It is recommended that ISPs use current best practice standards and resources in determining whether a customer's computer is compromised. Examples include but are not limited to:

(a) Review mail queues and network traffic patterns for anomalies or known patterns of bot/malicious activity;

(b) "Ingress" and "egress" address validation and spam checking;

(c) Gateway IPS/IDS;

(d) Internal firewall systems;

(e) Internal systems used to identify well known Trojans/viruses using well known TCP and UDP port numbers;

(f) Reports from customers.

(g) Microsoft makes sources of information (data on potentially compromised computers) available to ISPs through their SNDS service, refer to: https://sendersupport.olc.protection.outlook.com/snds/

2. **Banking industry**

There is a dedicated CSIRT serving the banking industry with a specific email address to be used by ISPs subscribing to the iCode: ispa@bankcsirt.org

3. **Other sources of information**

There are also external sources of compromises / malicious activity which an ISP may choose to use, such as:
(a) Spamcop reports;

(b) DNSBL reports;

(c) SORBS reports;

(d) RBLS (Blacklist notification subscription);

(e) Internal Spamassassin scanning and reporting of outbound mail destined to popular spam target domains like Hotmail, Yahoo, BigPond;
(f) Reports from other organisations such as My Net Watchman, SpamCop, RoadRunner, JunkMail Filter, other ISPs and external individuals;

(g) Microsoft makes sources of information (data on potentially compromised computers) available to ISPs through their SNDS service, refer to https://sendersupport.olc.protection.outlook.com/snds/

(h) IETF recommendations for the Remediation of Bots in ISP Networks, refer to https://datatracker.ietf.org/doc/rfc6561/

A cyber security incident involving unauthorised access to or impairment of electronic communications, for example a denial-of-service attack, may constitute an offence under the Electronic Communications and Transactions Act 25 of 2002 and/or the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2000. There are also specific forms of cyber security incidents which may trigger an obligation on an ISP to notify a government agency once the ISP becomes aware of such incidents.

Note that ISPs are not generally obliged by law to monitor their networks for the purpose of identifying criminal or unlawful conduct.

4. Law Enforcement

There is currently no specific SAPS contact available for ISPs: where a crime is committed against the ISP this needs to be reported to your local SAPS station bearing in mind this advice. SAPS Station Finder - https://www.saps.gov.za/contacts/index.php

Issues relating to children, including grooming and child sexual abuse material can be reported to childprotect@saps.gov.za or using the key contacts for the (FCS) Family Violence, Child Protection and Sexual Offences unit - https://www.saps.gov.za/contacts/keydetail.php?id=121