



# **CODE OF ETHICS**



For INFORMATION SECURITY PROFESSIONALS

## THE NEEDS OF CODE OF ETHICS FOR INFORMATION SECURITY PROFESSIONALS



- Many of the international professional bodies such as GIAC, EC Council and ISC<sup>2</sup> use the code of ethics to provide benchmark to their professional members for self evaluation and also to establish a framework for professional's behavior and responsibilities.
- Looking into scenario in Malaysia, there are many people acquired their information security professionals through mastering the intellectual skill, training, education and experience without receiving certification from the well-known international professional bodies. However, these information security professionals do not have any common framework of ethical that they can channel or attach themselves to.
- Therefore, this paper proposes the Code of Ethics that can be adopted by the group of information security professional described above. In fact, any new established information security professional associations or organizations can adopt this proposed code of ethics as their standards professional conduct and practice to provide guidance to their members in conducting a day-to-day works and services.



### **OBJECTIVES**

The **Code of Ethics for Information Security Professionals** are established with the objectives:

- To guide information security professionals on how to align behavior, action and decision with highest standards of professionalism
- To provide a benchmark for information security professionals to use for self evaluation
- 3. To minimize problems with ethical behaviors and encourages responsible behavior
- 4. To help professionals identify and resolve the inevitable ethical dilemmas that they will confront during the course of their information security career.





#### WHO IS THE INFORMATION SECURITY PROFESSIONAL?

Based on the *Institute of Information Security Professional* (IISP), information security professionals are distinguished by certain characteristics as follows:

- 1. Mastery of a particular information security skill, acquired by professional training, education, certification, experience or combination of them
- 2. Adherence by its members to a common set of values; and
- 3. Acceptance of a duty to society as a whole.





#### THE INSTILL VALUES

The Code of Ethics for information security professionals is derived from Unified Framework for Information Security Professionals which emphasized on 3 core ethic values; Integrity, Objectivity and Professional Competence & Due Care which required all members to observe:

VALUES	DESCRIPTIONS
Integrity	Perform duties in accordance with existing laws and exercising the highest moral principles
	Refrain from activities that would constitute a conflict of interest
	Act in the best interests of stakeholders consistent with public interest
	Act honorably, justly, responsibly, and legally in every aspect of your profession
Objectivity	Perform all duties in fair manner and without prejudice
	Exercise independent professional judgment, in order to provide unbiased analysis and advice
	When an opinion is provided, note it as opinion rather than fact



## THE INSTILL VALUES (cont...)

VALUES	DESCRIPTIONS
Professional	Perform services diligently and professionally
competence and due care	Act with diligence and promptness in rendering service
	Render only those services which you are fully competent and qualified
	<ul> <li>Ensure that work performed meets the highest professional standards. Where constraints exist, ensure that your work is both correct and complete within those limits. If, in your professional judgment, resources are inadequate to achieve an acceptable outcome, so inform clients and principals</li> </ul>
	Be supportive of colleagues, and encourage their professional development.  Recognize and acknowledge the contributions of others, and respect the decisions of principals and co-workers
	Keep stakeholders informed regarding the progress of your work
	Refrain from conduct which would damage the reputation of the profession, or the practice of colleagues, clients, and employers
	Report ethical violations to the appropriate governing body in a timely manner



#### **CODE OF ETHICS**

Derive from the 3 core ethic values, the following are the code of ethics that consist of 7 guiding principles (GPs) where the information security professional shall adhere to:

GUIDING PRINCIPLES (GP)	DESCRIPTIONS
GP 1: Act all times in accordance with existing laws,	Do not engage in unethical or unlawful acts that negatively affect the community, professional reputation, or the information security discipline
association values and exercising highest moral principles	<ul> <li>Act with fairness and justice to all parties and refrain from activities that would constitute a conflict of interest or damage the reputation or detrimental to information security profession or association</li> </ul>
	Act in best interest of stakeholders consistent with public interest



GUIDING PRINCIPLES (GP)	DESCRIPTIONS
GP 2:  Protect and maintain appropriate level of confidentiality, integrity and availability of sensitive information in any course of professional activities	<ul> <li>Respect the confidentiality of information acquired during the course of their duties</li> <li>Do not use or disclose, share, disseminate or distribute any confidential or proprietary information without proper and specific authority or unless there is a legal or professional requirement to do so</li> <li>Avoid misusing any confidential information for personal gain</li> <li>Treat all information received from a client or employer as confidential unless such information is in the public domain</li> <li>Take appropriate steps to minimize or mitigate potential risks, including recommending the engagement of another professional if need arises</li> </ul>



GUIDING PRINCIPLES (GP)	DESCRIPTIONS		
GP 3:	Exercise independent professional judgment, in order to provide		
Conduct the service with	unbiased analysis and advice		
fairness, courtesy and	Exercise restraint when commenting upon the work of other		
good faith towards clients,	members		
colleagues and others,	Do not maliciously injure the character or the prospects of  business of another member or individual, being as careful with		
give credit where it is due	business of another member or individual, being as careful with a colleague's reputation as with their own		
and accept, as well as			
give, honest and fair			
professional comments			



GUIDING PRINCIPLES (GP)	DESCRIPTIONS
GP 4:  Do not engage in any crimes or improper practices	<ul> <li>Do not engage in any crimes such as bribery, identity theft, forgery, fraud, financial crime such as credit card fraud or double billing or any other improper practices</li> <li>Reveal the conflict or any possible crimes without delay to the clients or employers, including interests (direct or indirect) held by close associates, relative and companions</li> </ul>



GUIDING PRINCIPLES (GP)	DESCRIPTIONS
GP 5: Perform all professional	Be responsible to safeguard the credibility and trustworthiness in rendering services
activities and duties in accordance with the highest	<ul> <li>Render only those services for which they are fully competent and qualified</li> </ul>
ethical principles	<ul> <li>Do not engage or be a part of any malicious activities that may harm others</li> </ul>
	Conduct services in the most ethical manner without prejudice



GUIDING PRINCIPLES (GP)	DESCRIPTIONS
GP 6:  Avoid professional association with those whose practices or reputation might diminish the profession	<ul> <li>Refrain from any activities that can damage the reputation and profession of yourself, or the practice of colleagues, client, and employer</li> <li>Report ethical violations to the appropriate governing body if needs arise</li> </ul>



GUIDING PRINCIPLES (GP)	DESCRIPTIONS
GP 7: Provide service with competence, honesty and forthrightness about limitations, experience and education	<ul> <li>Provide a guideline to those involved in the industry and maintain uniform ethical standards, and uphold the trust and welfare at all times</li> <li>Be aware of the exact nature and scope of professional activity and does not go beyond professional specificity</li> <li>Demonstrate personal commitment to ongoing professional development and building capability</li> </ul>





#### **SANCTIONS**

Any complaint must relate to actions or activities that have occurred within the last 12 months. It is important that most complaints should be dealt within 6 months and a maximum of 12 months period.

The sanctions, which the Disciplinary Committee can impose, are:

- Warning
- Severe warning
- Suspension
- Expulsion
- Fine





#### MAINTENANCE TO CODE OF ETHICS

Having a code is not enough to ensure ethical behavior. The code needs to be understood, used, taught, monitored and regularly re-evaluated and revised.

Therefore, any changes to the Code of Ethics and the associated disciplinary procedures must be agreed by the management of association.

The Disciplinary Committee can make recommendation to the board of association in this regard.





#### **CONCLUSION**

By establishing a set of guiding principles called Code of Ethics by which to work, it shall set a standard for information security professionals apart from others who may claim to provide similar service.

This Code of Ethics shall continuously be reviewed to ensure its relevancy.





#### **REFERENCES**

- GIAC Code of Ethics. Retrieved from: <a href="http://www.giac.org/overview/ethics.php">http://www.giac.org/overview/ethics.php</a>
- ISC2 Code of Ethics. Retrieved from: <a href="https://www.isc2.org/ethics/default.aspx">https://www.isc2.org/ethics/default.aspx</a>
- ISSA Code of Ethics. Retrieved from: <a href="http://www.issa.org/page/?p=17">http://www.issa.org/page/?p=17</a>
- Ethics Working Group. Retrieved from: <a href="http://www.ethics-wg.org/framework.html">http://www.ethics-wg.org/framework.html</a>
- Code of Professional Conduct & Practice. Retrieved from: <a href="http://www.mncc.com.my/code.htm">http://www.mncc.com.my/code.htm</a>
- ISACA Code of Professional Ethics. Retrieved from: http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx
- Ethical principles and information professionals: theory, practice and education. Retrieved from: <a href="http://www.alia.org.au/publishing/aarl/33.2/full.text/iacovin\_o.html">http://www.alia.org.au/publishing/aarl/33.2/full.text/iacovin\_o.html</a>
- Six Steps to Creating an Ethical Culture. Retrieved from: http://knol.google.com/k/six-steps-to-creating-an-ethical-culture#

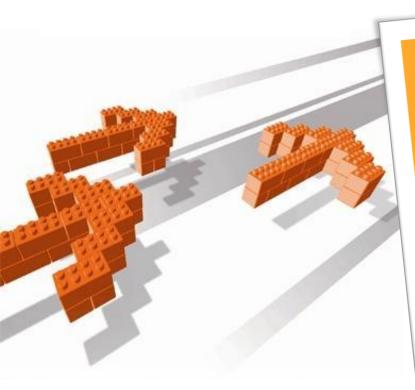
- Ethics Resource Center National Ethics Surveys.
   Retrieved from:
   <a href="http://www.ethicsworld.org/ethicsandemployees/nbes.php">http://www.ethicsworld.org/ethicsandemployees/nbes.php</a>
   #new09
- Ethical Issues for IT Security Professionals. Retrieved from: <a href="http://www.windowsecurity.com/articles/Ethical-Issues-IT-Security-Professionals.html">http://www.windowsecurity.com/articles/Ethical-Issues-IT-Security-Professionals.html</a>
- 11. Professional Ethics. Retrieved from:
  <a href="http://www.onepetro.org/mslib/servlet/onepetropreview?id">http://www.onepetro.org/mslib/servlet/onepetropreview?id</a>
  =ASSE-04-714-1&soc=ASSE
- Study: Ethical breaches becoming common in government. Retrieved from:
   http://www.govexec.com/dailyfed/0108/013008ar1.htm
- 2009 National Business Ethics Survey Ethics & Employee Engagement. Retrieved from: <a href="http://www.ethics.org/nbes/">http://www.ethics.org/nbes/</a>





An agency under MOSTI





Corporate Office:

CyberSecurity Malaysia,

Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia.

**Tel.** +603 8946 0999 **Fax.** +603 8946 0888 **Hotline.** +1 300 88 2999

www.cybersecurity.my

## Thank You



Best Brand Internet Security 2008 & 2009



CERTIFIED TO ISO/IEC 27001:2005 CERT NO.: AR4656



MS ISO/IEC 17025 TESTING SAMM NO. 456



