# Asia University Personnel Information Security Management Regularity

2009.12.28 Approved by the 5th OICT Advisory Committee
2010.02.09 Issued by Asia Mi Tze No. 0990001088
2011.11.09 Approved by the 9th OICT Advisory Committee
2012.01.18 Amended and Approved by the 6th Administration Committee of the 2011 Academic Year
2012.02.21 Issued by Asia Mi Tze No. 1010001358

1. The aim of this regularity is to implement the information security operation, keep confidentiality, completeness and availability of information and equipment as well as maintain all internal operations.
2. This regularity is applied to all administration personnel.
3. If not specified in this regularity, it can be applied to the following.
   A. Regularity of Computer Processing Personal Data Management for Private School and Academic Research Institute.
   B. Copy right law.
   C. Guidelines of Information Security Management for Executive Yuan and related Units.
   D. Personal Data Protection Act.
4. All personnel has to keep the secret for what he knows in the process of working and he cannot release the sensitive information to others.
5. Any data, needed for the official business, which is related to personal information or secret data cannot release to others unless the request has been applied and you are authorized to do it.
6. The important secret documents or contracts should keep in the safe place. If the document needs to be transferred, it should be sealed in the envelope so that the unauthorized persons cannot touch it or view the contents.
7. Passwords should be set for personal computer devices and application systems. The password selections have to follow the setup guidelines.
8. Using the password should bear in mind the following guidelines:
   A. Protect the password and keep it confidential: The user should change his password every six months, do not use the same password repeatedly.
   B. Do not write down the password on a paper or post it on a computer, monitor, and other easy-access locations.
   C. Whenever you think the system or password is encrypted, you have to change the password right away.
   D. The password should be at least six in length and follow the setup guidelines.

E. The password setup guidelines: Avoiding using the guessable or open information as follows
   i. Personal name, date of birth, ID number.
   ii. Organization name symbols or related issues.
   iii. User ID, user name, group user symbols or other system symbols.
   iv. Computer hostname, OS name, user name.
   v. Phone number.
   vi. Vocabularies on English or foreign language dictionary.
   vii. Terminology
   viii. Space

9. Set up screensaver rules on the computer. It will be activated if the device is not used for more than ten minutes.
10. Do not install illegal software on the computer. The device administrator is responsible for any possible legal actions.
11. The device user or administrator takes full responsibility for the system and information security. If the computer has got viruses or shows evidence of abnormality, you have to notify the personnel immediately.
12. All electronic data should back up regularly so that the business operation will not be affected because of malfunction of machine or human factors.
13. The personnel should obey this regulation, otherwise, the faculty members will be reported to Faculty Evaluation Committee; the administration staff, the Personnel Committee; the student, the Student Reward and Disciplinary Committee.
14. This regulation is approved by the Administration Committee, issued by the president. For the amendment, the process is same.