Tzu Chi University of Science and Technology Computer Equipment Security and Information Confidential Maintenance Rules

I. To ensure computer equipment security,information confidential maintenance and enhanced information operation control of all of the department, specially set up this rules.

II. Information confidentiality refers to the use of computer equipment to create and store information related to personal data files, and systems, programs, messages or documents related to the processing of such information.

III. All departments of the school shall take safety measures for computer equipment and information confidential, and their relevant supervisors shall be responsible for supervising within the scope of their powers and responsibilities.

IV. The school should establish a personal data and information security audit system. Depending on the need, audit personnel should be set up. Each unit should set up personal data and information security management personnel to check the use of computer equipment and information file management on a regular or irregular basis.

V. The computer server room should be designated to be responsible for management, and strengthen access control and related security measures.

VI. For the computer equipment of the uni/faculty, it should strengthen the protection against natural disasters, other accidents, computer viruses and malicious network intrusion, and set the power-on password and screen protection device.

VII. For media such as disks and tapes that store confidential information or software, a specialist should be assigned to manage them.

VIII. A backup system should be established. For long term or important archives, special fire protection or insurance equipment should be used for off site storage.

IX. All of the data should include the name and title of the executor should be recorded in detail and managed by a special person. Changes, deletions, use cases, etc. after the filing of the above documents shall be recorded.

X. Important or confidential information in each room should be recorded and backed up. If technical assistance is needed from the computer center, Application for Copying Hard Disk Data shall be filled and agree with the relevant personnel.

XI. The input and output of each data shall be established with the identification code and the management system of the pass code; when important or confidential data is filed, data access control shall be added.

XII. Connection should limit the scope of its operation in the system.

XIII. The computer program and its design, testing, production, use and maintenance should be strictly controlled.

XIV. The content of the previous article refers to the standard of program instructions, work control language, program change application form and program. When the information relating to the campus database is transferred, it is required to be approved by the principal.

XV. For the production of the program, an auditing procedure should be established, which is reviewed by the non-original-designer when the programming is completed.

XVI. If the function of transferring the school database data from a faculty/unit is not provided, and wanted to request assistance from computer, the related faculty needed to request the approval from principal in the signature way. Within five working days after receiving the signature, the computer center shall export the materials approved by the signature and submit it to the faculty/unit for the remaining related processes such as data sorting, proofreading, transfer or upload.

XVII. Principal will be invited after the approval to announce the implementation time of this approach via executive meeting.