Yuan Ze University
Cyber Security and Personal Data Protection Guidelines

Approved at the 6th Administrative Meeting of the 112th Academic Year dated October 18, 2023

Article 1 Yuan Ze University (hereinafter referred to as "the University") has formulated the following guidelines to uphold a comprehensive level of information and personal data security and to reinforce the secure management of diverse information assets, ensuring their confidentiality, integrity, availability, authenticity, and non-repudiation. Additionally, the University is committed to supporting the use of various application systems by faculty, staff, and students while safeguarding their associated personal data, all in accordance with operational requirements.

Article 2 These guidelines for information security and personal data protection at the University (hereinafter referred to as "the Guidelines") and various supplementary regulations established in accordance with these guidelines are formulated by referring to the Information Security Management Act, Personal Data Protection Act, information security management regulations of the educational system, and other relevant standards.

Article 3 These guidelines are applicable to all information assets and their users at the University. Users are required to strictly adhere to them, and violations will be subject to relevant legal measures.

Article 4 Definitions of terms used in these guidelines are as follows:

4.1 Information Security: This refers to safeguarding information assets from various threats, including unauthorized access, disclosure, alteration, theft, destruction, and more, with the aim of reducing the potential damage that could impact the operations of the University.

4.2 Information Assets: This encompasses the data and files collected, generated, and used by the University and the associated equipment necessary for these tasks.

4.3 Personal Data: This pertains to data that can directly or indirectly identify an individual, such as their name, date of birth, national identification number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical history, healthcare, genetics, sexual activities, health checks, criminal records, contact information, financial status, and social activities.

4.4 Personal Data Files: These refer to the compilations of personal data that are automatically retrieved and organized by machines or through non-automated means as established by the system.

Article 5 To honor individual rights regarding their personal data, including the right to inquire or request access, copies, supplementation, correction, cessation of collection, processing, use, and deletion, a contact point must be established to assist individuals

in addressing these matters and related complaints and inquiries.

Article 6 The University must implement appropriate security measures to prevent the theft, disclosure, alteration, destruction, or loss of personal data. In the event of a confirmed breach of personal data, emergency response measures must be promptly activated, and the affected individuals must be informed in an appropriate manner.

Article 7 To protect the security of information assets, each unit is required to maintain an inventory of information assets, categorize them, and establish corresponding control measures.

Article 8 The University must establish and implement a personal data protection management system to ensure the execution of personal data protection management. Regular reviews should be conducted for continuous improvement. After establishing or amending the personal data protection management system, it should be publicly announced within the University for effective implementation.

Article 9 When third-party vendors or organizations have access to personal data-related information of the University, the contracting unit should sign a confidentiality agreement with the other party and diligently supervise the entrusted party.

Article 10 The Regulations are implemented after being passed at the Administrative Meeting, and the same procedure applies to any future amendments.

Note: If any controversies or disputes occurred regarding clauses of the aforesaid regulations, it shall always refer to its Chinese version.