Yuan Ze University Cyber Security Plan

Version Number: 1.0

Date of Formulation: October 18, 2023

Yuan Ze University Cyber Security Plan

Table of Contents

I. Basis and Purpose

This plan is formulated in accordance with Article 10 of the Cyber Security Management Act and Article 6 of the Enforcement Rules of Cyber Security Management Act.

II. Scope of Application

This plan is applicable to all organizations within the University.

III. Core Businesses and Significance

1. Core Businesses and Significance

Core Business	Core Cyber System	Significance	Impact of Service Disruption	Maximum Tolerable Downtime	Protection Level
Network Services	External and Local Network Services	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Disruption of external and campus network services	8 hr	High
	DNS	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based	Inability to connect to specified servers or to resolve URLs	10 hr	High

		on the organization law and recognized as important			
	DMZ	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Server farm network disruption or reduced security protection level	16 hr	High
	Wireless Network Services	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Disruption of campus wireless network services	16 hr	High
Email Services	AD Services	□ Designated as critical infrastructure by the competent	Inability to provide account and password authentication,	9.5 hr	Medium

		authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	rendering all dependent servers inoperable		
	Virtual Storage Services	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Inability to store large capacity data	12 hr	Medium
	Front-end/Back-end Email Services	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by	Inability to provide email access, causing interruption in internal and external communication channels	12 hr	Medium

		the competent authority ■ Managed by the university based on the organization law and recognized as important			
	SPAM Filters	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Inability to provide email access, causing interruption in internal and external communication channels	12 hr	Medium
Homepage Services	Power Support Network Virtual Server Services	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Inability to use front-end WWW web services	11 hr	Low

	Power Support Network Virtual Server Services AD Services	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Inability to use back-end WWW web services	72 hr	Low
Backup System Services	Backup System	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Inability to provide automated backup services	12 hr	Low
Administrative System	Database Management	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the	Database damage, rendering information system inoperable	12 hr	Low

		cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important			
	Information System Operations	□ Designated as critical infrastructure by the competent authority □ Involves businesses subject to the cyber security responsibility level C designated by the competent authority ■ Managed by the university based on the organization law and recognized as important	Abnormalities in Web/client operating systems, affecting system processing results	8 hr	Low

2. Non-core Businesses and Details (as per the Table Below)

Non-core Business	Impact of Service Disruption	Maximum Tolerable Downtime
Department and Research Unit Websites	Potential partial disruption of department and research unit operations	24 hr
Client Services	Inability of administrative and faculty staff across departments to use network and printing services, etc.	24 hr

IV. Cyber Security Policy and Objectives

1. Cyber Security Policy

To enhance the information security management of the University and protect the information environment from intentional or unintentional threats, both the internal and external, and unauthorized access, use, control, disclosure, damage, alteration, destruction, or any other form of compromise, while ensuring confidentiality, integrity, and availability of data, the following policy is formulated for all university members to follow:

(1) To establish a risk management mechanism for cyber security and regularly assess the effectiveness of risk management in response to changing cyber security situations.
(2) To safeguard the confidentiality and integrity of sensitive information and cyber systems, preventing unauthorized access and tampering.
(3) To ensure authorized users can access information and cyber systems when needed.
(4) To comply with legal and regulatory requirements.
(5) To evaluate the impact of various man-made or natural disasters and create recovery plans for core cyber systems to ensure the continuity of core business operations.
(6) To reinforce the resilience of core cyber systems to ensure the continuous operation of university business.
(7) To respond to changing cyber security threats by providing cyber security education and training to enhance the awareness of cyber security among university members, who should actively participate in these training sessions.
(8) To introduce appropriate penalties for individuals involved in matters related to breaching cyber security within their business operations.
(9) To avoid clicking on emails from unknown or unidentified senders.
(10) To prohibit the sharing of a single cyber system account among multiple users.

2. Cyber Security Objectives

(1) Quantitative Objectives

i. To ensure a data center maintenance service availability of over 97% during the entire work year.
ii. To maintain a Level 4 cyber security incident-free status throughout the year.
iii. To achieve click and attachment viewing rates of less than 10% and 6% in the email social engineering exercise, respectively.
iv. To ensure employees meet the training-hour requirements of the Cyber Security Management Act according to their roles and responsibilities, reaching a 100% compliance rate.

(2) Qualitative Objectives

i. To strengthen internal controls to prevent unauthorized access and ensure the appropriate protection of information assets.
ii. To achieve compliance with cyber security responsibility level requirements and reduce exposure to cyber security risks.
iii. To ensure that all information security incidents and suspected vulnerabilities are reported through appropriate mechanisms, investigated, and addressed.

(3) Approval Process for Cyber Security Policy and Objectives

The University, in accordance with the “Organizational Regulations for the Yuan Ze University Cyber Security and Personal Data Protection Steering Committee,” should conduct an annual review of the information development strategy and plans along with the cyber security policies and objectives of the University. Once approved, these should be submitted to the Administrative Meeting for review and final approval by the President.

(4) Dissemination of Cyber Security Policy and Objectives

The Cyber Security Policy and Objectives will be communicated to all personnel and stakeholders, including IT service providers, through written documents, email, website announcements, or other appropriate means. Their effectiveness in implementation should be evaluated.

(5) Regular Review Process for Cyber Security Policy and Objectives

The Cyber Security Policy and Objectives should be reviewed annually, to make appropriate revisions in the event of changes in the organization, business, laws, or environmental factors.

V. Cyber Security Promotion Organization

In accordance with the "Organizational Regulations for the Yuan Ze University Cyber Security and Personal Data Protection Steering Committee," a Cyber Security and Personal Data Protection Promotion Committee should be established to facilitate relevant activities.

VI. Allocation of Dedicated Personnel and Funds

1. Allocation of Dedicated Personnel and Resources

(1) In compliance with the Cyber Security Responsibility Level Classification system, the University is categorized under Cyber Security Responsibility Level C. As a minimum requirement, the appointment of one dedicated cyber security professional is necessary. This professional is responsible for the following tasks:

i. Cyber security management: Overseeing activities related to protection requirements for cyber systems, implementation and verification of cyber security systems, content cyber security audits, institutional cyber security maturity assessments, and education and training.

ii. Cyber system security management: Managing tasks, including the classification and protection standards of cyber systems, security testing, and business continuity exercises.

iii. Cyber security protection: Handling responsibilities related to the management of cyber security monitoring mechanisms, introduction of government configuration standards, establishment of cyber security protection facilities, and promotions of cyber security incident reporting and response.

iv. Compliance with cyber security management regulations: Ensuring the execution of obligations under the Cyber Security Management Act within the University.

(2) The responsible unit (Library and Information Service Center) of the University should engage in human resource activities related to cyber security and should focus on enhancing the training of cyber security personnel and elevating the cyber security management skills of the cyber security professionals of the University. If any relevant units lack sufficient cyber security personnel or experience when performing cyber security tasks, they may seek advisory and consulting services from scholars, experts, or professional institutions as needed.

(3) The development of professional competencies for dedicated cyber security personnel, such as obtaining certificates, licenses, and training records, should adhere to the provisions of the Regulations on Classification of Cyber Security Responsibility Level. Each professional should hold at least one cyber security professional certificate and one cyber security competency assessment certificate.

(4) University staff members, responsible for the management, maintenance, design, and operation of critical cyber systems, should have clearly defined roles and responsibilities. Those entrusted with maintaining confidentiality should sign written agreements, and personnel rotations should be implemented when necessary to establish a human resource backup system.

(5) Leaders and managers at all levels of the University should assume responsibility of overseeing the cyber security operations of their subordinates and prevent any unlawful and inappropriate activities.

(6) The allocation of professional human resources should be subject to annual reviews and integrated into the management review process of the continuous improvement mechanism within the cyber security plan.

(7) To comply with the requirements of the Cyber Security Management Act, the University should allocate one dedicated cyber security professional. Currently, the University assigns personnel who handle cyber security tasks concurrently. To meet

regulatory requirements, the University will proactively pursue dedicated cyber security positions in the future. The higher supervisory authorities are also hoped to provide budgetary support to fulfill the regulatory requirements for personnel allocation.

2. Allocation of Funds

    (1) When planning the allocation of resources and funds, the budget committee of the University should consider the information development strategies, plans, and cyber security policies and objectives of the University. It should ensure the provision of necessary resources for the establishment, implementation, maintenance, and ongoing improvement of the cyber security plan.

    (2) Units planning the development of cyber systems should incorporate the cyber security protection requirements into their overall budget and allocate a reasonable portion of the budget to cyber security.

    (3) If units have requirements for cyber security resources, they should align their requests with the budget planning schedule of the University and submit them to the budget committee for allocation. Once approved, they can proceed with the relevant implementations based on the overall allocation of cyber security resources.

    (4) The allocation of cyber security funds and resources should undergo regular annual review and be integrated into the management review of the continuous improvement mechanism within the cyber security plan.

VII. Inventory of Information and Cyber Systems

1. Inventory of Information and Cyber Systems

    (1) An annual inventory of information and cyber assets should be performed as per the "Information Asset Management Procedures" and compile an "Information Asset List" based on the inventory results.

    (2) The classification of cyber system protection requirements should be annually assessed, either internally or through outsourcing, in accordance with the "Regulations on Classification of Cyber Security Responsibility Levels" for Class C government agencies and the guidelines provided in Appendix Nine, "Principles for Classifying ICT System Protection Requirements."

    (3) Visible labels should be affixed to important information and cyber system assets. The labels should include particulars, such as asset numbers, custodian information, brand, model, and other relevant details. For core cyber systems and associated assets, additional labeling is required.

    (4) An annual review of the "Information Asset List" and the "Cyber System Inventory" should be performed to maintain their accuracy and completeness.

2. Classification of Institutional Cyber Security Responsibility Levels

The University, owing to its operation of self-developed or outsourced cyber systems, is classified as a Class C-level organization in terms of cyber security.

VIII. Cyber Security Risk Assessment

To create a framework for risk assessment and management within the information security management system, this document offers common risk assessment standards for the accountable units involved in information flow, custody, and usage at the University. This framework enables the effective implementation of risk control, mitigation of threats to information security, and establishment of procedures for risk assessment and management.

For more detailed information, refer to the "Risk Assessment and Management Procedures Manual" of the University.

IX. Cyber Security Protection and Control Measures

Based on the results of the cyber risk assessment (outlined in the previous section), protection standards for core cyber systems, and required tasks for cyber security responsibility levels, relevant protection and control measures should be implemented. Noteworthily, the core cyber systems of the University have already obtained ISO 27001 certification, and the specific details of protection and control measures can be found in the ISMS documents. Additional required tasks are as follows:

1. Business Continuity Exercises

A business continuity plan for core cyber systems should be developed, and regular exercises should be conducted at least once a year.

2. Security Testing

Periodic cyber security technical scans should be performed, including host vulnerability scans, web vulnerability scans, and penetration testing.

3. Cyber Security Health Checks

In accordance with the "Regulations on Classification of Cyber Security Responsibility Levels," a cyber security health check should be conducted every two years, and improvement measures should be developed based on the results.

4. Cyber Security Protection Equipment

(1) Antivirus software, network firewalls, and email filtering devices should be established and maintained to ensure regular updates or necessary hardware upgrades.

(2) Backups of log records should be periodically created from cyber security equipment, scheduled reviews should be conducted, execution should be audited by supervisors, and performance should be assessed.

X. Cyber Security Incident Reporting, Response, and Exercise Mechanisms

To promptly manage cyber security incidents and minimize their impact, the University has developed associated reporting, response, and exercise mechanism. For detailed information, refer to the "Cyber Security Incident Management Procedures" of the University.

XI. Assessment and Response to Cyber Security Intelligence

Upon receiving cyber security intelligence, the university must evaluate the content, considering its impact on the institution, acceptable risk levels, and available resources. Subsequently, the most appropriate response strategy should be chosen. When required, adjustments can be made to the control measures within the cyber security plan, and records of these actions should be maintained. The assessment and responses to different categories of intelligence are outlined as follows:

1. Cyber Security Intelligence

This category includes significant threat indicators, information about cyber security threat vulnerabilities and attack methods, analysis reports of major cyber security incidents, shared experiences concerning cyber security-related technologies or topics, and information about suspected system weaknesses or questionable programs. All of this information falls under the category of cyber security-related information.

After the compilation of such intelligence by the Cyber Security and Personal Data Protection Promotion Committee, a risk assessment should be conducted. Based on the results, the appropriate risk mitigation measures should be implemented according to the control measures specified in the cyber security plan.

2. Intrusion Attack Intelligence

A subcategory of cyber security intelligence, which includes specific instances, such as confirmed attacks on particular web pages, confirmed inappropriate content on specific web pages, confirmed personal data breaches on specific web pages, confirmed intrusions into specific systems, or identified network attack activities by specific systems, is referred to as intrusion attack intelligence.

Qualified cyber security professionals should evaluate the presence of immediate risks and, when necessary, initiate immediate reporting and response measures. Furthermore, they should implement corresponding risk mitigation measures outlined in the cyber security plan. Concurrently, relevant departments should be notified to strengthen preventive actions.

3. Sensitive Information Intelligence

Cyber security information may comprise personal data that can directly or indirectly identify individuals, such as names, dates of birth, national ID numbers, passport numbers, characteristics, fingerprints, marital status, family details, education, occupation, medical records, health information, genetic data, sexual activities, health check records, criminal records, contact information, financial status, social activities, and other data relevant to individuals, legal entities, or business secrets or operations of a group. The disclosure or provision of this information could potentially infringe upon the rights or legitimate interests of government agencies, individuals, legal entities, or groups, and may involve general government secrets, sensitive information, or national secrets. This type of information is classified as sensitive information.

In cases involving personal data, business secrets, general government secrets, sensitive information, or national secrets, employing methods, such as masking, deletion of specific sections or text, or the application of de-identification techniques for exclusion, is vital. This ensures the protection and confidentiality of such sensitive information.

4. Intelligence Related to Core Business and Core Cyber Systems

Intelligence within the realm of cyber security that encompasses core business data specific to the University, core cyber systems, or content pertinent to the functionality of key infrastructure that maintains core business or core cyber systems falls under the category of intelligence relevant to core business or core information and communication systems.

The Cyber Security and Personal Data Protection Promotion Committee is responsible for evaluating the potential impact of intelligence associated with core business or cyber systems on the University operations. The Committee should subsequently enact appropriate risk management measures in accordance with the cyber security plan.

XII. Management of Outsourced Cyber Systems or Services

To safeguard the security of outsourced operations at the University, a management procedure for outsourced systems and services has been established. For more details, refer to the “Management Procedure Manual for Outsourced Systems and Services” of the University.

When the University outsources the establishment and maintenance of cyber systems or the provision of cyber services, it should carefully consider the professional capabilities and experience of the service provider, nature of the outsourced project, and requirements for cyber security. Additionally, monitoring the cyber security maintenance provided by a service provider is crucial.

1. Considerations for the Selection of Service Providers
    (1) Service providers must implement comprehensive cyber security measures for the processes and environments of the outsourced services or have obtained third-party verifications.
    (2) Service providers should have an adequate number of qualified personnel, who have received proper training, hold information security professional certifications, or possess similar expertise in the field of information security.
    (3) The conditions under which service providers are permitted to subcontract the outsourced operations, scope and targets of subcontracting, and cyber security maintenance measures required for subcontractors should be explicitly defined.
2. Considerations for Monitoring the Cyber Security Maintenance of Service Providers
    (1) If the outsourced operation involves custom cyber system development, service providers should provide third-party security testing certificates for the developed system. In cases involving the use of non-self-developed systems or resources, service

providers should specify the non-self-developed content, its source, and provide authorization evidence.

(2) Service providers must immediately notify the contracting entity and take corrective actions when they violate cyber security regulations or become aware of cyber security incidents.

(3) Upon the termination or dissolution of the outsourcing relationship, service providers should ensure the return, transfer, deletion, or destruction of data held in compliance with the outsourcing agreement.

(4) Service providers should also implement other cyber security maintenance measures.

(5) The University should regularly conduct audits or use appropriate methods to verify the execution of the outsourced operations, especially when cyber security incidents that may impact the outsourced business are detected.

XIII. Cyber Security Education and Training

1. Requirements for Cyber Security Education and Training

To ensure the comprehensive security management and education and training of all employees, with the aim of minimizing information security incidents resulting from insufficient awareness, various categories of personnel have been assigned with distinct education and training requirements in accordance with the "Regulations on Classification of Cyber Security Responsibility Levels." These requirements are outlined as follows:

Personnel Category	Course Category and Duration
Cyber security professionals	Each member is required to undergo a minimum of 12 hr of cyber security professional training or cyber security skills training annually.
Information personnel excluding cyber security professionals	Each member is required to complete a minimum of 3 hr of cyber security professional training or cyber security skills training every two years, in addition to at least 3 hr of cyber security general education and training annually.
General users and supervisors	Each member is required to participate in at least 3 hr of cyber security general education and training annually.

2. Cyber Security Education and Training Modes

(1) The University should annually assess the requirements of different job categories, encompassing management, business, and information roles, to develop a comprehensive cyber security awareness and education and training plan. This plan is designed to instill a strong understanding of cyber security among employees and elevate overall cyber security standards of the University. Records pertaining to cyber security awareness and education and training should be maintained.

(2) The content of the cyber security awareness and education and training plan should include:

i. Cyber security policies (including the contents of the cyber security plan, management procedures, processes, requirements, personnel responsibilities, and procedures for reporting cyber security incidents).

ii. Cyber security legislations.

iii. Cyber security operational procedures.

iv. Cyber security technical training.

(3) During the on-board program, new employees should receive thorough orientation regarding the cyber security operational regulations of the University and their significance.

(4) The policy for cyber security education and training should be universally applicable to both the employees and external users of the University.

XIV. Assessment Mechanism for Public Agency Personnel Engaged in Business Related to Cyber Security

The regular assessment and employment procedures for the University personnel should be conducted in compliance with the Cyber Security Rewards and Penalties Regulations for Government Personnel and the pertinent provisions outlined in the human resource policy of the University.

XV. Continuous Improvement and Performance Management Mechanism for the Cyber Security Plan and Its Execution

1. Execution of the Cyber Security Plan

To effectively execute the cyber security plan and ensure the efficient functioning of cyber security management within the University, relevant departments must align their various documents, processes, procedures, and control measures with the cyber security policies of the University, objectives, and the content specified in this plan. Additionally, they should maintain records of the relevant execution results.

2. Audit Mechanism for the Execution of the Cyber Security Plan

(1) Implementation of the Audit Mechanism: The Cyber Security and Personal Data Protection Audit Team should conduct internal audits within the University. Audit results must be reported to relevant management levels, including the Chief Cyber Security Officer. Records of the audit process should be retained as evidence for cyber security audit plans and audit events.

(2) Audit Improvement Report:

i. After the audit, when deficiencies or areas for improvement are identified, the audited unit should develop improvement measures, plan the improvement progress, and ensure their implementation.

ii. After the audit, when deficiencies or areas for improvement are identified, the audited unit should determine the reasons behind them and assess the presence of similar deficiencies or areas for improvement.

iii. After identifying the reasons for deficiencies or areas for improvement, the audited unit should propose and implement relevant improvement measures and progress plans. When necessary, making changes to the current cyber security management system or related documents should be considered.

(3) Continuous Improvement and Performance Management of the Cyber Security Plan:

i. The Information Security Committee should hold cyber security management review meetings at least once a year to confirm the execution of the cyber security plan, ensuring its ongoing appropriateness, suitability, and effectiveness.

ii. Management review topics should include the processing status of previous management review cases, changes related to internal and external issues associated with the cyber security management system, feedback on cyber security performance, the results of risk assessments and the progress of risk control plans, handling and improvements of significant cyber security events, stakeholder feedback, opportunities for continuous improvement, the appropriateness of revisions for the cyber security plan, and the execution of the cyber security plan.

iii. Records of the management review for the continuous improvement mechanism should be compiled into meeting minutes and properly maintained, which serve as evidence of the management review process.

XVI. Reporting of the Execution of the Cyber Security Plan

In accordance with Article 12 of the Cyber Security Management Act, the University is obliged to conduct an annual external audit or provide reports at designated intervals to the higher authorities. This is to apprise them of the execution of the cyber security plan, ensuring that they are well-informed about the annual cyber security plan implementation of the University.

XVII. Related Regulations, Procedures, and Forms

1. Related Regulations and Reference Documents
   (1) Cyber Security Management Act
   (2) Enforcement Rules of Cyber Security Management Act
   (3) Regulations on Classification of Cyber Security Responsibility Levels
   (4) Regulations on the Notification and Response of Cyber Security Incident
   (5) Cyber Security Information Sharing Regulations
   (6) Cyber Security Rewards and Penalties Regulations for Government Personnel
   (7) Organizational Regulations of the Cyber Security and Personal Data Protection Promotion Committee of Yuan Ze University

2. Related Forms
   (1) Document Inventory
   (2) Information Asset List
   (3) Corrective and Preventive Actions Form
   (4) Confidentiality Agreement with Contractors
   (5) Confidentiality Agreement for the Employees of Contractors
   (6) Internal Information Security Audit Plan
   (7) Internal Information Security Audit Form
   (8) Internal Information Security Audit Report

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