National Yang Ming Chiao Tung University Regulations Governing Information System Security

Approved at the fifth Administrative Meeting for the 2020–2021 academic year on June 2, 2021.

Approved at the first meeting for the Information Security and Personal Data Protection Promotion Committee for the 2021–2022 academic year on June 20, 2022.

Amended at the first Administrative Meeting for the 2021–2022 academic year on September 14, 2022.

1. The National Yang Ming Chiao Tung University Regulations Governing Information System Security (hereinafter referred to as “the Regulations”) were established by National Yang Ming Chiao Tung University (hereinafter referred to as “the University”) to maintain the confidentiality, integrity, and availability of the University’s information systems and to prevent malicious intrusions.
2. Divisions that intend to operate self-developed public information systems shall submit system development security documents and vulnerability scan reports related to their systems to the IT Service Center (hereinafter referred to as “the Center”). Systems approved by the Center and deemed not to be of high or medium risk can be officially launched. For each system that does not meet the criteria, the Center shall provide a vulnerability verification report to the system management unit and notify the unit of improvements that need to be made before the deadline.
3. Divisions that intend to outsource the development of their public information systems should require the outsource party to deploy sufficient and properly qualified and trained cyber security professionals who hold cyber security professional licenses or have similar business experience, in accordance with Article 4 of the Enforcement Rules of Cyber Security Management Act
4. Divisions that intend to outsource the development of their public information systems should evaluate potential risks prior to commissioning contractors for the development of information systems. Additionally, each division should sign off on the appropriate information security protocols with each contractor to ensure that the contractor complies with the relevant information security regulations of the University and assumes full responsibility for such compliance. Please see the additional clauses to the contractual responsibility of

contractors related to information security (Appendix 1).

5. During the contracted period, the system authority of the contractor should be adequately monitored and revoked immediately upon completion of the contract period.

6. Each division should implement regular reviews of their self-developed or commissioned information system based on the principles of classification and the defense standards stated in the Regulations on Classification of Cyber Security Responsibility Levels.

7. The main information system of each division must be protected by a firewall or other information security infrastructure to monitor data transmission and access in external and internal networks and to prevent intrusion and destruction, tampering, deletion, and unauthorized access within the system. In addition, the applicability of the control policies for the firewall should be regularly reviewed.

8. The Regulations shall be implemented after approval by the Administrative Meeting. The same rule shall apply to all subsequent amendments.

Appendix 1: Additional clauses to the contractual responsibility of contractors related to information security

Article 1:

Contractors granted access to the websites, information services, and system maintenance (hereinafter referred to as “IT services”) of National Yang Ming Chiao Tung University (hereinafter referred to as “the University”) must comply with the information security regulations of both the University and its competent authorities.

Article 2　Information security requirements of contractors:

(1) Contractors should provide the University with a vulnerability scan report and system development security documents for review before handing over IT services. The IT Service Center of the University (hereinafter referred to as “the Center”) retains the right to randomly perform vulnerability scans, the criterion for which no high or medium risk should be detected. Contractors are recommended to use credible software for vulnerability scanning, such as Nessus, OWASP-ZAP, OpenVAS, or Acunetix.

(2) Contactors should attach documents related to information security when handing over IT services. These documents should include a vulnerability scan report and system development security documents. The system development security documents should include contents related to the information security control functions of the IT system, including password hashing, account management, access control measures, separate frameworks for websites and databases, risk analyses and countermeasures, code security assessment, system backups, and restoration plans.

(3) Contractors shall be held fully responsible for the information security of the software and all digital documents (e.g., those stored on USB drives or hard disks) handed over to the University. Therefore, contractors should inspect for malicious entities (e.g., worm viruses, Trojan viruses, spyware) and covert channels before handing over software or digital documents to the University. For the handing over of IT services, contractors must clear all testing-related data before uploading the services to the relevant official online environment.

(4) Contractors shall comply with the Cyber Security Management Act of Republic of China and the requirements specified in the Regulations and make improvements in any areas where the regulations have not been met before the deadline. Failure to make such improvements shall result in an official notification from the University stating that the IT service in question shall be blocked or taken down. Violations to the requirements shall be handled according to the disciplinary measures specified in

the contract.

(5) During the maintenance period, contractors must comply with the requirement of conducting annual vulnerability scan tests to ensure that the IT system is not at high or medium risk of violation. In addition, website services must be protected through data encryption and pass the test of the Center before registration under the domain of the University.

(6) All IT services handed to the University shall be subjected to regular auditing, vulnerability scanning, and penetration testing throughout the quality assurance and service period. If any anomalies are detected, the Center may take information security countermeasures, including auditing, vulnerability scanning, and penetration testing. The costs incurred from any such countermeasures shall be paid in full by the contractor.

(7) If a contractor is required to perform maintenance or management of the host computer from an external source, the contractor must first submit an application to the Center. After evaluation and approval of said application by the competent authority, the contractor shall be granted access.

(8) After a contract has been closed or terminated, all information related to the University held by the contractor during the service period shall be deleted or disposed. In addition, contractor shall sign the Personal Data Return and Destruction Affidavit Letter, and records of all such instances of deletion or disposal shall be retained.

(9) All IT services provided by contractors (e.g., software or system development) must implement version management. Additionally, IT services shall provide access management and access record retention functions in accordance with the regulations related to information security.

(10) Contractors shall retain records pertaining to the handling of anomalies for the Center to review if necessary.

(11) If any changes occur among the personnel responsible for system development, contractors shall actively contact the University and return any borrowed equipment, software, or operational authority to the University.

Article 3　Information security responsibility of contractors:

(1) All contractors who engage in or handle IT services shall sign a non-disclosure agreement or affidavit and uphold their responsibility to maintain confidentiality.

(2) All contractors must comply with the Personal Data Protection Act of Republic of China and the University's regulations related to personal data protection to ensure the security of the University's data and personal privacy data (e.g., data related to any person's name, date of birth, ID Card number, features, fingerprints, marital status, family information, educational background, occupation, health conditions, medical records, financial status, community activities, phone number, or residency). If the University suffers damage or loss as a result of operational negligence on the part of an employee of the contractor, the contractor shall be held responsible for the damage or loss incurred (including any data leaked from websites managed by the contractor).

(3) Regarding the occurrence of information security events during the service period of a contractor, the contractor must immediately notify the Center or the relevant competent authority, propose emergency countermeasures, and comply with the subsequent handling procedure(s).

(4) If any of the IT services delivered to the University by the contractor involves the use of systems or resources that are not developed by the contractor itself, it shall be marked as not self-developed content and provide the source and its proof of authorization. In case of infringement the legal rights (e.g., intellectual property rights) of a third party, the contractor shall be responsible for handling and bear all legal responsibilities.

Article 4　Other precautions:

(1) If a contractor turns over any IT services or products to a subcontractor or subcontractors for support, the contract must specify the authority–responsibility relationship between the contractor and the subcontractor (as detailed in the contract wording or specified in the contract appendices) to assure the overall deliverable level of service quality of the contractor is achieved. Subcontractors must also comply with the Regulations.

(2) If contractors must bring laptops or portable data storage media (e.g., floppy disks, CD-ROMs, USB drives, external hard drives) to use in the Center's Computer Center, they must first receive the approval of the accompanying personnel responsible, and any employees of the contractor must be registered on the visitor list of the Computer Center. The visitor list of the Computer Center shall be regularly reviewed by the relevant competent authority.