NATIONAL TAIWAN UNIVERSITY
Directives for Accessing Security Camera Footage, License Plate Recognition Data, and Building Access Records

February 16, 2016 Passed by the 2,893rd Administrative Meeting
November 10, 2020 Deliberated, amended, and passed by the 3,081st Administrative Meeting
July 20, 2021 Deliberated and passed by the 3,098th Administrative Meeting

Article 1 National Taiwan University (NTU or "the University") formulates the NTU *Directives for Accessing Security Camera Footage, License Plate Recognition Data, and Building Access Records* ("the Directives") to ensure regulatory compliance in its processing and use of campus security camera footage, license plate recognition data, and building access records (collectively, "the system data"), as well as to safeguard the rights and interests of its faculty and students.

Article 2 Except for the system data located in the Administration Building and other buildings, as well as the roads surrounding them, which shall be retained by the Campus Security, all other security camera footage, license plate recognition data, and building access records shall be retained by the competent unit that utilizes the data ("data retention unit").

The system data shall include historical data generated prior to a given incident as well as real-time data generated on the day of the incident.

Article 3 Except where expressly stipulated by law or otherwise requested by law enforcement via an official document, access to the system data shall be limited to incidents involving public affairs, security, and order at the University so as to prevent infringements of personal privacy and violations of the *Personal Data Protection Act*.

In addition to the provisions of the preceding paragraph, access to real-time data shall only be granted to University staff or government agencies entrusted with the relevant powers who require such access in the course of their legal duties, or in matters that pose imminent danger to the lives, persons, freedom, or property of faculty members and students.

Article 4 Faculty and staff members and students who wish to review the system data shall visit Campus Security to fill out an application form, which shall indicate the reason for and purpose of the application, the beginning and ending time of the data needed, and the location of the system. The application form together with supporting documents shall be submitted to the data retention unit for approval.

In addition to the provisions of Article 3 herein, non-NTU persons who wish to review the system data shall submit an official letter from law enforcement or a police report filing in order to apply. Alternatively, they may apply in the presence of a law enforcement officer, who must produce a form of identification.

Applicants shall vouch for the accuracy of the information provided in the application form as well as the supporting documents, and shall be held accountable for any legal liability arising from fabricated or falsified information.

Article 5 Upon approval of the application, the relevant data retention unit shall assign a person to review the requested data with the applicant, or provide such data in the form of a compact disc or a printed copy for Campus Security, who shall review the requested data with the applicant.

Applicants may request preservation of the system data described in the preceding paragraph, in which event the data retention unit shall store the data in a compact disc or flash drive and submit it to Campus Security for custody. Under no circumstances shall such data be taken off the premises of the University.

In principle, only government agencies and internal units of the University with legal investigation authority may request a copy of the system data. Faculty and staff members, students, and non-NTU persons who wish to request a copy of the system data for evidence preservation purposes or other legally mandated investigative procedures shall apply to the data retention unit by providing an official letter issued by the competent government agency.

Article 6 Persons who handle the system data are prohibited from unauthorized accessing, recording, photographing, or copying of any such data in any way. They shall keep the system data confidential and may not disclose or deliver it to any third party. The University may hold violators accountable in accordance with the law and seek indemnification for any damages resulting therefrom.

Article 7 Data retention units may not in any way disclose or deliver the system data to anyone who is not authorized to review or copy such data. The University may hold violators accountable in accordance with internal regulations and seek legal redress and indemnification in accordance with the law.

Article 8 The Directives shall be passed by the Administrative Meeting and then implemented.