NATIONAL TAIWAN UNIVERSITY
Directives for Handling Unusual Network Activity

September 03, 2014 Passed by the Administrative Meeting of the Computer and Information Networking Center
September 02, 2021 Passed by the Administrative Meeting of the Computer and Information Networking Center

Article 1 The National Taiwan University (NTU or "the University") Computer and Information Networking Center ("the Center") formulates the NTU *Directives for Handling Unusual Network Activity* ("the Directives") in accordance with Article 6 of the University's *Campus Network Usage Regulations* to ensure information security and uninterrupted network service on campus.

Article 2 The Center may take the following measures as necessary when it receives reports of suspected intellectual property infringement, information security incidents, or unusual network activity:

1. The Center shall forward any official letters sent by external organizations to the academic program or unit (collectively, "the competent unit") with which the equipment or user in question is affiliated. The competent unit shall inform the external organization in question of the handling results via official letter, a copy of which shall be addressed to the Center. If any relevant evidence is provided by the external organization via email or other means, the Center shall forward it to the competent unit, which shall inform the Center of the handling results.
2. The Center may suspend the campus network access of the equipment from which the unusual activity originates. The Center shall disclose the IP address of the equipment and the reason for its disconnection from the network on the NTU Information Security Center website.
3. The competent unit shall notify the administrator of the equipment to remove any copyright-infringing materials or resolve the equipment issue.
4. In the event of suspected intellectual property infringement, the competent unit shall resolve the issue and then notify the Center to restore the equipment's access to the campus network. For information security incidents or unusual network activity, the network administrator of the competent unit shall resolve the issue and then restore the equipment's access to the campus network.

Article 3 In the event of a suspected information security incident, the affected unit shall take the following measures as necessary:

1. The unit shall notify the Center immediately and submit an Information Security Incident Report within one hour of becoming aware of the incident.
2. The Center shall then handle the incident in accordance with the Ministry of Education's *Information Security Reporting and Response Procedures* based on the typology and severity of the incident.

Article 4 Those who wish to create a whitelist of usage exceptions for educational or research purposes in the information security equipment deployed by the Center shall submit a project proposal with a specified project timeline and then apply to the Center upon approval of the head of their academic program or unit. The whitelist shall become effective upon review and passage by the Center.

Article 5 The Directives shall be passed by the Administrative Meeting of the Center and then implemented on the date of promulgation.