National Chengchi University IoT Devices Security Guidelines

Passed at the 18th meeting of the Information Security and Personal Data Protection Implementation Committee on October 31, 2022

I. The term "IoT Devices" as mentioned in these guidelines (hereinafter referred to as “the Guidelines”) refers to devices equipped with network connection capabilities for managing official operations, including wireless network base stations/wireless routers, IP cameras, network printers, access control devices, environmental control systems, digital players, drones, etc.

II. Units shall establish a management inventory of IoT devices and update it at least once a year.

III. Device must incorporate a security update mechanism to ensure that their overall protection remains intact.

IV. Device shall include an identity authentication mechanism, and the default password provided by the vendor and any easily guessable passwords must be avoided. **Default passwords must be changed**. The password length should be at least eight characters, using a combination of two of the following elements: uppercase and lowercase English letters, numbers, and special symbols.

V. Unneeded network connections and services shall be disabled for the Device, and appropriate network access restrictions shall be set based on operational needs; a firewall must be established for Device that do not require external connectivity, ensuring that only internal connections are permitted.

VI. Where the security control specifications in Articles 3, 4, and 5 of the Guidelines cannot be implemented for Device, a compensatory control mechanism shall be established and Internet connection capabilities shall be restricted, strengthening access control or monitoring network connection behaviors. If Device has known vulnerabilities that cannot be patched or updated, a timeframe for replacement shall be established.

VII. According to regulations of the Executive Yuan, the use of information and communication Device from Chinese manufacturers is prohibited.

VIII. Device shall be evaluated and tested in accordance with the Guidelines before being purchased.

IX. When purchasing IoT devices, preference shall be given to IoT devices that have received the IT Security Label, and an information security-related agreement shall be signed with the Device supplier. The content of such

agreements shall include service commitments, security update periods, and proactive reporting of known security vulnerabilities in the Device; the agreement shall also propose relevant response plans and clearly state relevant responsibilities.

X. Regarding the use of Device in NCCU’s rental venues, outsourcing contracts or venue rental usage regulations shall clearly stipulate that products endangering national security (such as software, hardware, and services from Chinese manufacturers) must not be used.