<u>**CSU Fullerton Asset Acceptance Agreement**</u>

The CSU, Fullerton Rollout program is providing a laptop and/or iPad for faculty and certain staff members. This program addresses the need by faculty and staff members to have a laptop and/or iPad in addition to a desktop computer. The laptop and/or iPad provided is for university related business as a productivity tool, curriculum tool, and a research and communication tool. It is not to be used as a personal computer or a replacement for any computers or mobile device that may be owned personally. The laptop and/or iPad is state property, and must be used in conformance with the terms and conditions of applicable software license agreements. It may not be used for personal purposes.

I.   Responsibility for Damage, Loss or Theft

It is the faculty/staff member's responsibility to take appropriate precautions to prevent damage to or loss/theft of his or her laptop and/or iPad. Information Technology will not repair or replace the laptop and/or iPad unless the cost of repair/replacement is paid by either the department or the individual user.

If the laptop and/or iPad is lost or stolen it must be reported to: the local police, the campus information security officer, and Information Technology (IT) - Help Desk (657-277-7777). A copy of the police report must be sent to IT- Help Desk as soon as possible. The police report should include the serial number, CSUF property tag number, and a description of the protected data (see section VI) of the lost/stolen laptop and/or iPad. A loss or theft of University issued equipment form must also be filled out and returned to IT- Help Desk.

II.   Upgrades and Troubleshooting

If a laptop and/or iPad requires hardware upgrades (e.g., memory, peripheral, or hard disk), software installation, or has problems that cannot be resolved over the telephone, the laptop and/or iPad will need to be brought to the IT- Help Desk for hardware service, software installation, or problem diagnosis. IT- Help Desk staff will not visit a home or go to off-campus locations to provide services.

Modifying your iPad and/or laptop is prohibited. An iPad that has been modified will not be supported and the user is financially responsible for an un-usable iPad and/or laptop due to any modifications performed.

III.   Software Licensing

The laptop and/or iPad will be configured with a standard suite of programs that are appropriate for the type of computer the user received based upon the campus software standards. It is also possible that other applications will be provided to the user by the University based upon the professional needs or the requirements of the laptop. The University has policies for appropriate use of software, including the requirement to demonstrate legal license to a program before it can be installed on University owned equipment.

IV.   On/ Off Campus Internet Access

The laptop and/or iPad is equipped with wireless connectivity that allows you to access the Internet on and off campus. Users must comply with all University policies, particularly computer and internet guidelines, when using the laptop and/or iPad.

March 12, 2019

V.   Backup

You are responsible for backing up and maintaining the data on your university issued rollout laptop and/or iPad. Documents and data files on the laptop and/or iPad are not backed up or stored on any University hardware, and the University is not responsible for the loss of documents or files from the laptop and/or iPad. If you have questions about backing up your laptop and/or iPad documents or files, please contact the IT- Help Desk.

VI.   Virus, Hacking, and Security Protection

To ensure that virus protection and other security patches are current, laptops and/or iPads are managed by JAMF and SCCM/Intune management client for Apple and PC devices respectively. No attempt to remove, alter or otherwise tamper with these management clients is permitted for any reason. If the management client is detected as removed it will be re-installed. Continued removal by the end user may result in device being revoked.

Users must take responsibility for ensuring that security updates take place on laptops and/or iPads in their care. In many cases devices must be restarted for updates to complete. Users will receive desktop pop up notifications when this is needed. In most cases users will have one week to comply with restarts unless a zero-day vulnerability is detected. Please do not ignore update notifications and take action on them as soon as possible.

Microsoft BitLocker and Apple FileVault are used to encrypt the data on campus laptops. Any electronic information that is classified by the University as "Protected Data" must be encrypted. If the laptop and/or iPad is lost or stolen and you believe any Protected Data is present, you must include these facts in your police report. For more information about Protected Data, please visit: www.fullerton.edu/it/iso/policy/

VII.   General Policies

You must not use your laptop and/or iPad to violate any state or federal law or CSU, Fullerton policy. You may not use the laptop and/or iPad for non-educational commercial purposes.

The above provisions are subject to revision by CSU, Fullerton. You will be informed of any changes. In the event of revision to the protocol you agree to conform to the revisions or to return your laptop and/or iPad to CSU, Fullerton. Laptop and/or iPad users should consult with their chair or supervisor if they have any questions about the appropriateness of any use or practice related to the laptop and/or iPad.

I acknowledge that I have read the above provisions and I will follow these protocols and policies.

_____   _____
Print Name   CSUF Property Tag Number

_____   _____
Signature   Date