ITS Telecommuting Agreement Addenda

NOTE: Numbers correspond to sections in the campus telecommuting agreement.

1. Proposed Work Schedule
   A. Standard university business hours (PST) should apply (accounting for time zone differences, etc.). Otherwise, the employee can have a separate agreement that sets an alternate work schedule as necessary.

5. While telecommuting, the ITS employee:
   A. Will remain accessible during the telecommute schedule, and understands that management retains the right to modify this agreement on a temporary basis as a result of a business necessity.
   B. Will check in with the supervisor to discuss status and open issues.
   C. Will be available for video conference and teleconferences, scheduled on an as-needed basis.
   D. Will be available to come into the office if a business need arises.
   E. Will request to use vacation, sick or other leave, which must be approved by the employees' supervisor in the same manner as when working at the regular University work site.
   F. Shall not be the primary caregiver of any children, adults or elders.

7. Regarding expenses incurred by the employee, ITS will not provide the following:
   A. The ITS employee is responsible for providing space, telephone, printing, networking and/or Internet capabilities at the telecommute location, and shall not be reimbursed by the employer for these or related expenses. Internet access must be via DSL, Cable Modem, or an equivalent bandwidth network. Issues related to individual tax deductions for the designated workspace in the employee's home or other remote location shall be the responsibility of the employee.

Additional ITS Requirements

The ITS employee will adhere to policies, standards and guidelines published by the University.

A. University policy assigns the ownership of the administrative records of the University to The Regents of the University of California. This applies whether such records are in paper, digital, or other format, and regardless of their physical location. University employees are required to provide the University with copies of records in their possession that pertain to the administrative business of the University. Additionally, records relating to the business of the University may be considered public records subject to release under the California Public Records Act and/or the Information Practices Act. University and non-University individuals are expected to comply with requests for copies of records in their possession that pertain to University business or as required by law.

B. All devices used for University business purposes are expected to comply with UC Minimum Security Standards (see https://security.ucop.edu/policies/security-controls-everyone-all-devices.html).

C. The ITS employee is expected to comply with the “ITS Policy Regarding Storage and Transmission of Personal Identity Information (PII)” (see http://its.ucsc.edu/policies/pii.html). If the employee uses or accesses university owned or created Personal Identity Information (PII), restricted data, or confidential data at a remote work site, this data must be protected according to UC policy, campus standards, and the law against malware and other threats of inappropriate access, disclosure, use, modification or destruction, on the computer, wherever the information is stored, when information is being transmitted, and in paper format. This requirement applies to all remote work activities, whether under a formal telecommuting agreement or not. Refer also to ITS’ Remote

Revised June, 2020
ITS Telecommuting Agreement Addenda

Access Requirements (http://its.ucsc.edu/policies/ra.html) and Security website (http://its.ucsc.edu/security), for additional details and guidance.