COVID-19 Pandemic

Sonoma State University Telecommuting Policy

Policy

In response to the COVID-19 pandemic and Declaration of Campus Emergency dated March 16, 2020, the University recognizes the value in facilitating telecommuting agreements for employees to increase the ability to ensure recommended social distancing guidelines. To this end, telecommuting will be authorized pursuant to this emergency policy. Appropriate Administrators should communicate this policy to all of their employees and are encouraged to explore options for their staff members to telecommute. This policy is subject to revision as the emergency unfolds.

Purpose & Scope

As a part of the University's response to the COVID-19 Pandemic, telecommuting is hereby authorized for non-faculty employees in order to align with the national goal of observing social distancing and to support the local shelter-in-place orders. The University acknowledges that not all jobs are suitable for telecommuting; however, the overall reduction of persons on campus contributes to the safety of employees who telecommute and those working on campus. All classifications of employees, (MPP, Confidential, represented members or student employees) are eligible for participation in the telecommuting program.

Telecommuting agreements are intended to provide the ability for employees to telecommute when it is reasonable to do so. Employees are not entitled to telecommuting agreements, and agreements may be suspended or terminated at any time by the University. The University will continue to observe the conditions of collective bargaining agreements not specifically superseded by this emergency policy.

Definition

Telecommuting is a specific work alternative program. This program provides the option of working at home or an alternate location, through a written agreement.

Authority

The Declaration of Campus Emergency dated March 16, 2020, authorizes the President to adopt emergency policies to ensure the safety of students, faculty, and staff. All valid telecommuting agreements executed during the University declared emergency will be valid until canceled by the University or until an institutional policy is approved through established processes.

Eligibility

Employees may participate in the telecommuting program through agreement between the employee and the Appropriate Administrator. All telecommuting agreements require the completion of a collaborative process to include the employee, Appropriate Administrator, and Human Resources. The agreements must be approved by the Appropriate Administrator, Associate Vice President/Dean (AVP/Dean), and Human Resources based on conditions established in the process.

Appropriate Administrators are encouraged to restructure employee duties and provide suitable work assignments to facilitate part- or full-time telecommuting. If any duties must be performed on-site, the

administrator will denote that on the request form. An Appropriate Administrator may deny a request to telecommute for employees considered essential. Essential employees will be given justification for the denial of the telecommuting request.

Equipment Provision & Responsibility

This policy authorizes a telecommuting program. For such purposes, the University does not bear the responsibility to provide an employee with a telecommuting agreement equipment required to accomplish the conditions of the agreement. An employee may use personally-owned equipment to participate in the telecommuting program. The employee is responsible for the care and maintenance of such equipment to include, but not limited to, computers, phones, and printers. Extraordinary costs may be approved for reimbursement on a case-by-case basis.

Indirect costs such as home maintenance, utilities, or maintenance and depreciation of personal equipment used while telecommuting is the responsibility of the participating employee.

Emergency conditions may mandate telecommuting because conditions exist that prohibit an employee's critical duties from being performed while physically at the University.

Responsibilities

Appropriate Administrators

Appropriate Administrators are responsible for ensuring a timely, fair, and reasonable assessment of any employee's participation in the telecommuting program. Generally, denial of the telecommuting request is only permissible when the nature of an employee's work is directly related to facility or equipment maintenance, direct and physical provision of care of students or employees, or access to systems or documents that cannot be reasonably or securely accessed remotely.

Appropriate Administrators who approve telecommuting agreements are responsible for ensuring the participating employee meets all expectations for quality and quantity of work and professionalism. Appropriate Administrators are to confer with Human Resources to identify and work to resolve performance or safety issues associated with telecommuting before suspending or terminating agreements.

Appropriate Administrators are responsible for ensuring adequate supervision by a management level employee (Management Personnel Plan [MPP]) for any employees within the work unit physically on-site if the assigned MPP is telecommuting. On-site MPP supervision may be arranged with another MPP in the same work unit, with the approval of the AVP/Dean. If an employee's Appropriate Administrator is scheduled to telecommute, that Appropriate Administrator will notify their employees of the on-site supervisor. The establishment of an on-site supervisor does not change the reporting structure for the unit nor does the assigned MPP relinquish management responsibilities.

Participating Employees

Participating employees are to provide accurate information in the collaborative process and to follow all conditions of an approved request. Employees must report any matters that alter their ability to comply with the conditions of the agreement to their Appropriate Administrator as soon as possible.

Participating employees must observe normal working hours (including rest and meal periods) as established in their agreement and remain available during those times to respond to inquiries by phone, email, or other means established by the agreement or to return to campus upon request and with

reasonable notice from the Appropriate Administrator to report for any matter that requires an in-person presence. Such appearance to campus is not considered travel and is not eligible for reimbursement.

Employees will be expected to observe appropriate social distancing and other public health guidelines when on campus.

Compliance with University Policies

Program participants shall comply with all applicable policies and procedures of the University and within the employee's department unless expressly superseded by this policy.

Technical Support

Information Technology (IT) will provide standard help desk support to program participants. Such support may require the employee to bring the device to the campus.

Information Security

Participating employees shall protect University information from unauthorized disclosure or damage and will comply with Federal, State, and University standards, policies and procedures regarding disclosure of public and official records. Work done at the program participant's off-site workplace is official University business. All records, documents, and correspondence, (either on paper or in electronic form), must be safeguarded and returned to the University at the conclusion of telecommuting or upon request by the employee's Appropriate Administrator.

Program participants must take reasonable and recommended precautions to ensure that their devices, whether University or employee owned, are secure before connecting remotely to SSU information assets and must close or secure connections to campus desktop or system resources (i.e. remote desktop, virtual private network connections, etc.) once they have completed University-related activities or when the device is left unattended.

Telecommuting employees agree to protect and maintain University Data in conjunction with Information Security policies. **Level One and Level Two data may only be accessed through VPN connections on devices.** VPN connections require IT assistance and requests will be managed based on IT resources.

Level 1 and Level 2 data may not be accessed using employee owned equipment unless they've worked with IT to establish a secure connection. Additionally, employees are not authorized to store University documents or work product on employee owned devices. All such material is to be stored in University supported cloud storage systems such as Google Drive.

Additional conditions to protect data will be specified in the Telecommuting Agreement, dependent upon the participant's duties.

Legal and Tax Implications

The participating employee is responsible for addressing and resolving any questions about the employee's ability to deduct expenses related to telecommuting. The tax implications of utilizing a home office are the responsibility of the employee.