USF Health Leadership Checklist for Telecommuting Preparation

- ✓ Determine under which circumstances telecommuting will be permitted (e.g., permanently, part-time, temporary).
- ✓ Communicate the telecommuting policy and procedures to employees and have them sign the telecommuting agreement.
- ✓ Identify the equipment necessary for employees to work remotely.
  - o Determine if employees will be permitted to use personal devices/home computers for business purposes.
  - o Determine if additional hardware must be purchased and identify the budget, funding source and timeline necessary for these items.
  - o Set up tracking system for USF equipment used remotely.
- ✓ Identify software needed for employees to work remotely and coordinate installation with IT.
  - o Designate a point of contact within the IT department to troubleshoot and assist remote workers.
  - o Ensure employees know how to access systems and files remotely.
  - o Determine what level(s) of access will be permitted to the organization’s networks and how access will occur. Ensure access is set up for a virtual private network (VPN), remote desktop or portal if needed.
- ✓ Develop home office guidelines for remote workers that may include the ability to:
  - o Make, receive and participate in phone and teleconference calls.
  - o Access the USF VMware platform.
  - o Follow all USF/USF Health security and computer standards, regulations, policies and procedures, including the safeguarding of proprietary information and PHI.
- ✓ Address timekeeping procedures for nonexempt employees, if these will differ for remote workers, and expectations for preapproved overtime work. Workers can remotely log into Kronos. Contact Payroll for instructions.
- ✓ Determine the training needs of supervisors and employees who are involved in remote work.
- ✓ Conduct a practice run if circumstances allow.
- ✓ Come up with a solid productivity plan/evaluation program that focuses on outcomes of the work, not physical presence of the employee.

USF Health