OSU CHS IT REMOTE WORK AGREEMENT

1. Equipment owned by Oklahoma State University Center for Health Sciences may be removed from the University campus to complete University-related business with the supervisor's prior approval and notification to the OSU CHS IT department. Supervisor must initiate a request to the OSU CHS IT Helpdesk once employee has been approved to work remotely.
2. The employee acknowledges University ownership of the equipment, support to this equipment will be conducted by OSU CHS IT personnel. Any configuration of software or work on the hardware must be performed by OSU CHS IT only.
3. The employee shall not connect or install personal peripheral devices such as printers, USB hubs, scanners, etc. on OSU CHS owned devices.
4. The employee must follow instructions from OSU CHS IT to keep equipment up to date while working remotely. If computer is taken off the OSU premises to work remotely, computer must be brought back to an OSU CHS location at least every 30 days and user must log on to computer while in the OSU Network to allow for various updates.
5. The University-owned equipment is to be used only for job-related activities and in compliance with OSU CHS Appropriate use and Security policies [Compliance - 9b- Information Technology - All Documents (sharepoint.com)](sharepoint.com).
6. The University-owned equipment will be returned to OSU CHS at the earliest of any of the following times:
   a. at the request of the employee's supervisor or other designated University representative;
   b. at the end of project for which the equipment is being used; or
   c. at the employee's termination of employment with the University.
7. The employee accepts responsibility for replacement of the University-owned equipment, listed below, in the event it is either lost, damaged, or destroyed, or is not returned to the University as described in #6 above.
8. If the University-owned equipment is either not returned to OSU CHS or is not in acceptable working condition, the employee authorizes OSU CHS to charge the employee's Bursar account for the cost of repairing or replacing the equipment.
9. The employee must have a high-speed internet connection (any broadband internet access such as cable or DSL) in place to be able to work remotely. The internet connection must be sufficient to adequately support video meetings. OSU CHS IT will not be responsible for supporting or troubleshooting the employee's internet connection.
10. The employee will not print from OSU CHS or personal computers while working remotely to protect regulated information such as PHI, FERPA, PCI.
11. The employee should notify their supervisor and CHS IT Helpdesk within one hour of any equipment malfunction or failure. In the event of such malfunction or failure, employee should make arrangements to bring their equipment and check with their supervisor about steps to be able to continue to work.
12. If employee will be using a personal device to connect to OSU CHS Network:
    a) Employee must have at minimum, the security controls listed below in place.
       - Supported operating system and automated updates in place on their device.
       - Antivirus software with automated scans enabled.
          - List of supported Operating systems and reputable Antivirus software can be found on the following link - [Working remote? | Oklahoma State University (okstate.edu)](okstate.edu)
       - Employee must not upload files from personal device on to the OSU CHS network unless file has been scanned for viruses.
    b) Employee must contact the OSU CHS IT Helpdesk to either bring personal equipment on site or connect remotely to validate security controls mentioned

above are in place. If these are not, employee must take action immediately and prior to connecting to the OSU CHS Network. OSU CHS IT will not assist in the installation or configuration of these security controls.

    c) OSU CHS IT will not be responsible for supporting/troubleshooting or installing any hardware or software on employee's personal device

    d) OSU CHS will not be responsible for damage or repairs to employee's personal device(s).

13. While connected to the OSU CHS network, the use of both OSUCHS provided equipment and personal equipment will be governed by OSU CHS Information Technology. The employee will be responsible for safeguarding all OSU CHS information and equipment and for ensuring that proprietary or confidential information is handled appropriately. This includes full compliance with HIPAA, FERPA, PCI regulations. The employee may not duplicate OSU CHS owned software as stated by the manufacturer's agreement.

14. The purchase of Hardware and Software for the purposes of supporting employee to work remotely must be done through OSU CHS IT, and department funds will be provided for the purchase of equipment and hardware, included but not limited to (Laptop, encrypted USB drive, keyboard, mouse, docking station, monitor, special software, etc.)

I have read and understand the following policies:
Appropriate Use Policy 3-0601
Remote Access Policy SEC-09.03
Information Security 3-0603

OSU Employee Name: _____

Equipment Description	Serial number	Asset/Tag Number

Off-Campus Location of Equipment: _____

      In signing below, I acknowledge that I have read this agreement and understand and agree to all the provisions.

_____
Employee's signature   Date

_____
Supervisor's signature   Date