



# JONES COUNTY

Department of Social Services  
Jessica Adams, Interim Director

## Temporary Teleworking Agreement

This Agreement is between the Jones County Department of Social Services ("JCDSS") and \_\_\_\_\_ ("you")

- A. We (JCDSS and you) agree that you will temporarily telework in accordance with a schedule set up and approved by your manager or supervisor.

You understand that this agreement is a temporary measure only and will be reviewed continuously during the period in which the State of North Carolina encourages social distancing. Accordingly, JCDSS at its discretion, may alter this schedule or end the temporary teleworking agreement at any time.

- B. You agree to maintain a presence with your Division/Section while temporarily teleworking. Presence may be maintained using the technology available such as by laptop computer, mobile phone, email, messaging application, videoconferencing, instant messaging and/or text messaging at all times during the times the Agency expects or requires you to work. You are expected to maintain the same response times as if you were at the offices of the Jones County Department of Social Services. You will make yourself available to physically attend scheduled work meetings as requested or required by the Agency.
- C. This temporary teleworking arrangement will begin with approval of the County Director of Social Services on \_\_\_\_\_ and will remain in effect unless altered or terminated at any time as described in paragraph A above.
- D. While temporarily teleworking, you will work just as if you were in your Regular Work Location and maintain productivity, performance, communication and responsiveness standards as if you were not temporarily teleworking. This Agreement does not change the basic terms and conditions of your employment at JCDSS. You will perform all of your duties as set forth in your job description, as well as and/or different duties that JCDSS may assign from time to time. Further, you remain obligated to comply with all Federal, State and, local policies and procedures.
- E. If you are a non-exempt employee, you are not to work overtime without prior approval from your supervisor, and you are required to take your rest and meal breaks while teleworking.
- F. You will be solely responsible for the configuration of and all of the expenses associated with your teleworking workspace.
- G. All injuries incurred by you during hours and all illnesses that are job-related must be reported promptly as prescribed by the Workers' Compensation Administration policy.

---

H. This Agreement and any attached Addendums contains the final and entire agreement and understanding between the Parties and is the complete and exclusive statement of its terms. This agreement supersedes all prior agreement and understandings, whether oral or written, in connection therewith.

I. By signing this Agreement, you are also confirming you have read, understood and will comply with all provisions listed above. You acknowledge that if your manager or supervisor determines that the temporary teleworking arrangement described in this Agreement is not working effectively or as envisioned, management may at any time adjust or end the temporary teleworking arrangement.

J. UNDERSTOOD AND AGREED:

Employee Signature \_\_\_\_\_

Print Name \_\_\_\_\_

Date \_\_\_\_\_

APPROVED BY:

\_\_\_\_\_  
Jones County Director of Social Services

Date \_\_\_\_\_

---

## **Addendum II: Confidentiality and Security**

### **Physical Security of Computers, Electronic, and Removable Media**

Computers and electronic media that receive, process, store, or transmit Confidential Information, including FTI, personally identifiable information and protected health information, must be in a secure area with restricted access. In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, the equipment must receive the highest level of protection practical, including full disk encryption. All computers and mobile devices that contain Confidential Information and are resident in an alternate work site must employ encryption mechanisms to ensure that this data may not be accessed, if the computer is lost or stolen. Confidential Information remains subject to the same safeguard requirements and the highest level of attainable security

Basic security requirements must be met, such as keeping Confidential Information locked up when not in use. When removable media contains Confidential Information, it must be labeled as containing Confidential Information. All computers, electronic media, and removable media containing Confidential Information, must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container.

Telework from a public place, such as a coffee shop, is not allowed. The home office must be in a separate room or area of the house with a physical barrier between the teleworker and other household members. Teleworkers are responsible for purchasing their own office furniture, such as desks, chairs, and lamps. Office supplies, such as paper and pens, are supplied by the agency. Printers are not provided, and staff must do their printing in the agency office. Confidential destruction of documents must only be done at the agency office.

Computer screens must not be visible to others. When not in use, computers must be safeguarded by double locks. The log-in password to open the computer is considered a lock, and an additional log-in to the office system or agency network may be considered a second lock. Best practice is to place laptops into a locked drawer or cabinet when not in use, or to have them anchored and locked to a desk. Confidential data should never be saved onto a computer desktop.

It is important to have a plan in place for unexpected disruptions to computer connectivity. These disruptions could be the work network, the internet service, or the teleworker's home computer. In the event of an outage, the teleworker must immediately contact his or her supervisor.

### **Equipment**

The agency retains ownership and control, for all hardware, software, and end-point equipment connecting to public communication networks, where these are resident at all alternate work sites. Employees also must have a way to communicate with their managers or other members of the agency in case security problems arise.