Office of Child Support
POLICY SHEET

SUBJECT

Alternate Worksite Policy **PS# 22-03**

POLICY

It is Office of Child Support (OCS) policy to safeguard information in its possession, including but not limited to Federal Tax Information (FTI), Social Security Administration (SSA) data, Personal Identifiable Information (PII), and Federal Parent Locator Service (FPLS) information. If the confidentiality of FTI, SSA, PII, and FPLS data can be adequately protected, telework sites such as employee's homes or other non-traditional work sites can be used. OCS will provide specialized training in security, disclosure awareness, and ethics for all participating employees and managers. This training will cover situations that could occur as the result of an interruption of work by family, friends, or other sources.

PROCEDURES

To ensure the security of information, either from the SSA, IRS directly or received through FPLS, is not inadvertently disclosed while working at an Alternative Worksite, it is OCS policy that all alternative worksites are set up and maintained with the following assurances:

- In situations when requirements of a secure area with restricted access cannot be maintained, such as home worksites, remote terminals or other office worksites, the state issued equipment must receive the highest level of protection practical, including full disk encryption.
- Staff shall confirm that they have access to a safe and comfortable workspace with the required level of security and necessary office equipment, including a telephone, in order to be approved to work from home.
    - Staff are required to be accessible via telephone and/or email during scheduled work hours.
    - Staff engaged in telework, must, unless otherwise authorized, devote their full time attention and effort to the duties and responsibilities of their position during scheduled work hours.
    - Staff engaged in telework shall not conduct personal business and/or pursuits, except to the limited extent permitted by state policy, during scheduled work hours.

- There shall always be two barriers to OCS case information, including but not limited to FTI, SSA and FPLS. When staff are not able to access the system through the state network directly, they will log in using GlobalProtect using multi-factor authentication.
- All computers, electronic media and removable media containing sensitive information obtained from FTI, SSA and FPLS must be kept in a secured area under the immediate protection and control of an authorized employee or locked up.
    - Staff shall never leave state issued laptops unattended except when secured in a locked space or shut down when inactive.
    - For those brief moments when employees step away from their computers, the laptop screens must be locked until they return.
- Staff shall maintain a clean desk surface/area in any alternative worksite, free of files, documents and related paperwork when they are not present and actively working in the designated workspace.
    - Any work-related materials taken to the alternative worksite location must be appropriately protected in compliance with the same security provisions which apply at the official duty station.
- Staff shall use headphones when needed to ensure that phone calls and discussions with our customers are not overheard by people/family members in a nearby vicinity.
- Staff shall disable any/all services that rely on unapproved information systems for audio and/or video recording, storage, or processing while working with FTI. Such systems are considered "external information systems" and use with FTI is prohibited under AC-20: External Information Systems. OCS requires the following when working with FTI in areas with such devices:
    - Treat such devices as if they are another person in the room because many such devices and applications can record and/or transmit data when activated. To protect FTI, staff must mute or disable the listening/detecting features of the device so that FTI data is not recorded.
    - If the device or application can take photos or record video or sound, then the employee must not do sensitive work within visual or audio range. These devices/applications include (but are not limited to the examples provided):
        - Digital assistances (such as Dot or Echo hardware using Alexa software, HomePod using Siri, etc)
        - Voice-activated devices and smartphone applications (such as Siri, Google Now ("Okay Google"), or Alexa on phones, tablets, etc.)
        - Internet-connected toys (Cloud Pet, Smart Toy, Hello Barbie, etc.) that might record or transmit
        - Security systems and webcams in the telework environment
        - Smart TVs or other equipment (if it includes voice activation), such as Peloton exercise bike
        - Operating systems/applications (such as Windows 10, Cortana, etc.) that allow voice commands and are not approved by the agency
        - Smart home and home surveillance, security, and video/audio devices: webcams on personal devices in the home, security cameras/microphones, smart thermostats with listening

    - If FTI inadvertently ends up on such an information system (IS) or device, the agency must follow its spillage procedures and incident response requirements in Publication 1075, Section 4.8.
- Information contained in ACCESS and other connected casework systems shall not be disclosed to unauthorized parties. Any unauthorized disclosures of information must be reported based on the Incident Response Procedure.

RATIONALE

The Agency of Human Services in Vermont has developed policy and procedures regarding teleworking that has been incorporated into this OCS policy sheet: AHS HR Procedure Manual-Telework

The Agency of Human Services in Vermont has also developed a Social Security Administration Data Protection Protocol that is reviewed and attested to by all State of Vermont employees on an annual basis, including OCS staff.

In addition, IRS Publication 1075 instructs OCS to have separate policy in place for an Alternative Worksite.

Date	Action	Description
10/27/2022	Created	
06/12/2023	Revised	Fixed hyperlinks and applied standard formatting
08/28/2023	Revised	Updated reference from Open VPN to GlobalProtect