Teleworking Requirements and Best Practices

Below are some excerpts from the TWC P-26 – Telecommuting Agreement and TWC Privacy Manual which involve safeguarding SPI.

Please substitute "TWC" or "agency" with what's most appropriate: **Provider** or **Board**, and/or delete what is not applicable for the Boards/Providers.

- All TWC-owned data, software, equipment, supplies, documents, and work product must be properly protected and secured.

- Policies regarding the protection of Sensitive Personal Information apply with full force while telecommuting. All documents, computers, and electronic storage containing SPI must be secured from unauthorized review at all times. This includes not sharing SPI with any person in your household who is not authorized to review the information.

- Employee agrees to designate a workspace within Employee's telecommuting location and maintain this workspace in a safe condition, free from hazards and other dangers to Employee and TWC equipment. The telecommuting location workspace must be free from unreasonable distractions and disturbances from children, pets, family members and others. The site is subject to approval by TWC.

- Employee agrees that TWC may make on-site visits to the telecommuting location for the purposes of determining that the site is safe and free from hazards, and to maintain, repair, inspect or retrieve TWC-owned equipment, software, data and/or supplies. In the event legal action is necessary to regain possession of TWC owned equipment, software, data and/or supplies, Employee agrees to pay all costs of such action including attorney's fees, should TWC prevail.

- By accepting TWC equipment, Employee acknowledges and accepts accountability and responsibility for such equipment. In the event of loss, misuse or theft of this equipment, Employee agrees to immediately (no later than 24 hours) report the loss, misuse or theft to Employee's supervisor, and Employee accepts the responsibility for the cost of changing or replacing said equipment if it is determined that Employee is at fault through negligence, recklessness, intent or otherwise for the loss or harm to the equipment.

Teleworking Requirements and Best Practices

- When not actively in use SPI must be in a secured compartment. For persons working at home, a secure compartment may be a closet, box or drawer that is within the control of the teleworker at all times in which the SPI is located within the home. In the control of the teleworker at all times means all exterior doors are locked when the teleworker is not at home or that the information is kept in a locked container (locked office), sealed envelope or taped box. If another person has access to the SPI without the teleworker being present, it is not in a secure compartment.

- Personally owned computers shall not be used to download, save, store, or host SPI. Use of a personally owned computer through an authorized method of connecting to TWC computer such as Microsoft 365, or VPN is permissible. Screen shots, or other local storage of SPI is forbidden.

Safeguarding laptops, tablets, smartphones, and other portable computing devices

Traveling, Transporting and Storage in Vehicles

- **Get it out of the car.** Don't leave your laptop in the car—not on the seat, not in the trunk. Do not leave your laptop in your car overnight. Take all work-related material (case files with SPI, laptops, smartphones) inside your residence or the hotel. Parked cars are a favorite target of laptop thieves; don’t help them by leaving your laptop unattended.

- **Treat your laptop/tablet like cash.** If you had a wad of money, would you turn your back on it—even for just a minute? Leave it on the backseat of your car? Of course not. Keep a careful eye on your laptop just as you would a pile of cash.

- **Mind the bag**. When you take your laptop on the road, carrying it in a computer case may advertise what’s inside. Consider using a suitcase (or a Pelican case), a padded briefcase or a backpack instead.

- **Don't leave it "for just a minute."** Your conference colleagues seem trustworthy, so you're comfortable leaving your laptop while you network during a break. The people at the coffee shop seem nice, so you ask them to keep an eye while you use the restroom. Don’t leave your laptop unguarded—even for a minute. Take it with you if you can, or at least use a locking laptop cable to secure it to something heavy.