Telework Best Practice: Protecting Sensitive Information

Teleworking and Information Security

Telework presents many benefits to the federal workforce, such as managing commutes, saving taxpayer money by decreasing government real estate, and ensuring continuity of essential government functions in the event of emergencies. While telework allows for greater flexibility in managing our workforce, there are risks to privacy and information security that are inherent with a remote workforce. Information security policies do not change when an employee works from home. It is the duty of the employee to safeguard Sensitive information, including personally identifiable information (PII), while teleworking.

Safeguarding Sensitive Information

Effective teleworking begins with having a signed telework agreement in place. Employees should work with supervisors to determine what types of documents are appropriate to take home and what documents should stay secured within the organizations work space. Know the sensitivity of the information, and make sure they are appropriately marked to help mitigate the risk of unauthorized disclosure.

One of the most effective ways to safeguard documents containing Sensitive PII is to keep electronic documents within the organizations network and to properly secure hard copy documents that are taken outside of the organization's work space. Stay within the network by logging in remotely through authorized remote connection methods, whether you use an organization-issued laptop or a personal computer. If working from a personal computer authorized, do not forward documents to personal email accounts as a way to avoid issues such as slow network connectivity or the inability to print. While there may be instances where you need to send information to an individual's personal account (i.e. job applicant), forwarding unencrypted emails to personal email account or sending unencrypted documents outside the organizations network that contain Sensitive PII is considered a privacy incident (or data breach).

When teleworking, identify the files needed to work on in advance, and organize them on network shares or organization laptops so that they will be easily accessible while teleworking. In addition, the use of organization-approved collaboration tools, such as SharePoint, to easily access files while teleworking is encouraged. However, before using collaboration tools to store Sensitive PII, make sure the tool has been approved for such use and that access is limited to only those individuals whose need for the information is related to his or her official duties. Have a back-up plan in mind in case issues are experienced with network connectivity, but never transfer files to personal computers using thumb drives or other portable electronic devices.

Be able to secure your organizational equipment and information at all times, including while transporting information home or while traveling. If equipment or documents must be left unattended, secure them (i.e. in the trunk of your car, in a hotel safe, etc.), but only for short periods of time. Inventory documents before teleworking, and ensure all documents are returned to the office.

When	Do	Don't	Why
Before you telework…	Plan to ensure that sensitive documents can be safely accessed remotely. Only use organizational approved devices and ensure these devices and their authorized connection methods are encrypted.	Don't forward emails to your personal email account or use non-approved portable devices. Have a back-up plan in case issues are experienced with network connectivity, but never transfer or download data to personal devices, personal email accounts, or to non-encrypted devices.	When you remove data from the organizations network, the organization cannot protect it. There may be instances where you need to send sensitive information to those without an organization account, but it must be encrypted. To send it unencrypted is considered a privacy violation.
	Obtain authorization from the organization to take home sensitive documents and make sure documents containing sensitive information in marked "confidential" or "privacy data." Inventory hard copies of documents taken from the office and when they are returned to the office.	Don't take sensitive information home that you do not need. Limit your removal of sensitive information from the office to only that information that is relevant and necessary to the work outlined in the telework agreement.	Hard copy documents are easily lost or misplaced, putting sensitive information at risk. Conducting an inventory and properly marking documents helps mitigate the risk of unauthorized disclosure.
Transport of documents…	Be able to secure sensitive information when not in use. If documents or devices containing electronic sensitive information must be left in a vehicle, lock them in the trunk, but only for short periods. When traveling, place sensitive information in hotel safe when not in use.	Don't leave your laptop or documents unattended overnight. Maintain accountability of data by ensuring documents are secured when not in use.	Failure to maintain accountability of sensitive information can lead to loss, theft, or misuse, resulting in a privacy violation.
At home...	Log in using authorized devices and connection methods. Organize home work spaces so that work files are separate from personal files and can be properly safeguarded.	Don't email or save files containing sensitive information to your home computer. Don't print agency records containing sensitive information to your home printer without authorization from the organization.	Home computers, printers, faxes, and copiers all contain internal storage or "hard drives." Even when these devices are disposed of, the information stored within is vulnerable.
	Leverage organizational collaboration tools such as SharePoint.	Do not post sensitive information on intranets, collaboration sites, shared drives, multi-access calendars, or on the Internet	Collaboration tools provide quick, easy access to data, but without proper security controls, can lead to data winding up in the wrong

	Access must be limited to those that have an official need to know.	(including social networking sites) that can be accessed by individuals who do not have a “need to know.” Don’t store sensitive information on collaboration sites unless target sites have been approved for such use.	hands. Sharing sensitive information with unauthorized users is considered a privacy violation.
	Secure sensitive information and ensure other household members do not have access to it. Organize work spaces at home so that government property and information are kept separate from personal property and can be properly safeguarded.	Don’t leave files containing sensitive information lying out in the open. Never leave sensitive information in view of children, spouses, or visitors. Sensitive information should be secured in locked cabinets and computers should remain locked when not in use.	Failure to properly secure sensitive information could result in inadvertent sharing of sensitive information.