

## GENERAL REQUIREMENTS

- An alternative worksite may be inside or outside the local commuting area of the bureau official worksite and is typically, although not always, the employee's residence.
- Remote work employees' locality pay is based on the location of their alternative worksite, which is their official worksite, and not the location of the agency's official worksite. Monetary impact of changes in pay is to be considered in decisions to allow or disallow remote work.
- If an employee is required to report to their agency's official worksite for meetings or other non-disciplinary business reasons and it is more than a 50-mile radius from their alternate worksite, they may be eligible to receive per diem and any applicable travel reimbursement. Monetary impact of travel expenditures is to be considered in decisions to allow or disallow remote work.
- Employees may work remotely from all 50 states, the District of Columbia, and Puerto Rico. **However, OSMRE management may limit the permissible area of remote work based on mission need and responsibilities.**
- Remote work cannot impact Essential Employee designations or responsibilities.
- Remote work employees are subject to the same performance requirements and standards of conduct as employees at the bureau's official worksite.
- Remote work cannot be used as an alternative for the employee to be the sole source of dependent care, (child or elder care) or to conduct personal business during work hours.
- Remote work employees have the same opportunities and requirements for training, awards, assignments and reassignments, promotion, reduction in grade, and retention as other employees. However, management may alter training options based on cost.
- Remote workers may, with their supervisor's approval, establish an alternative work schedule.
- During any period where OSMRE is operating under a continuity of operations or emergency plan, including, but not limited to, a pandemic or a terrorist or cyber-attack, the requirements of that plan supersede this Remote Work Program Directive.
- Remote workers are expected to follow OSMRE established protocol regarding security and confidentiality of information, including computer data and file security. Security measures in a remote work environment should cover information systems and technology, and all other aspects of the information systems used by the employee, including paper files, other media, storage devices, and telecommunications equipment (e.g., laptops, PDAs, and cell phones). Regardless of the worksite, it is the responsibility

of the employee to safeguard all sensitive information. Employees who engage in any type of remote work need to keep government property and information safe, secure, and separated from their personal property and information, but this is especially critical in a remote work environment. Federal employees should follow agency policies for managing records in a remote environment, such as returning files to the agency's filing system and managing copies of records created during remote working. Except for Bureau-specific policies, the general records management responsibilities of a federal employee do not change in the remote environment. Failure to comply with information security measures could result in the termination of remote work. For more information about an employee's records management responsibilities in a remote environment, please refer to the National Archives' Frequently Asked Questions about Telework.

- Temporary Duty (TDY) Travel Expenses. Payment of TDY travel expenses is determined by the employee's official worksite. The agency is responsible for travel expenses incurred by the remote worker for TDY travel away from the employee's official worksite. Therefore, management should consider the cost of business travel from the employee's requested remote location to other worksites or locations, as well as any travel to OSMRE office locations. Depending on the travel distance and frequency of travel, payment of TDY expenses may increase significantly.

## **RESPONSIBILITIES**

A. **Human Capital Officer** is responsible for:

- (1) Overseeing policy guidelines and developing requirements for implementing remote work arrangements within the Bureau.
- (2) Advising Bureau leadership on the administration and effectiveness of the OSMRE Remote Work Program.

B. **Associate CIO (ACIO)** is responsible for:

- (1) Developing strategies and providing guidance for enterprise information technology capabilities and data security required to support remote work arrangements.
- (2) Overseeing the evaluation of new and emerging technologies that facilitate remote work and approving them for -wide use, as appropriate.
- (3) Establishing criteria and guidelines for using and protecting government-furnished equipment (GFE) and non-GFE, including personally owned equipment to access OSMRE information systems and networks from a remote location and what printing is permitted from the remote worksite.
- (4) Reviewing and approving employee requests for overseas remote work arrangements.

C. **Regional Directors, Assistant Directors, HQs Office Chiefs** are responsible for:

- (1) Ensuring that their organizations are in full compliance with the requirements of this policy.
- (2) Establishing implementing procedures to govern the appropriate use of remote work arrangements as a work flexibility arrangement, to include integrating remote workarrangements into continuity of operations (COOP) plans.
- (3) Holding subordinate supervisors and managers accountable for implementing remote work arrangements in accordance with this policy guidance and applicable Bureau/Office implementing procedures.
- (4) Reviewing and approving employee requests for remote work arrangements, as applicable (including requested overseas arrangements).

D. **Supervisors** are responsible for:

- (1) Reviewing and approving remote work agreements with employees who request to and are permitted such arrangements; and terminating remote work agreements when arrangements fail to meet organizational needs.
- (2) Establishing and communicating clear expectations with employees approved for remote work arrangements regarding methods of communication (e.g., customer service, time frames for returning phone calls, email communication, etc.), meeting attendance, duty hours, and requesting leave.
- (3) Establishing clearly defined performance standards and using existing quality and quantity standards to evaluate work performance of a remote worker. Managing remote workers is similar to managing employees in the official worksite in that performance is measured by results.
- (4) Treating remote workers similarly as non-remote workers concerning performance appraisals, work assignments and requirements, awards and recognition, training and developmental opportunities, promotions, retention, and other employment matters involving management discretion; and treating employees equitably when implementing remote work arrangements in their organization.
- (5) Ensuring employees protect and secure agency records and sensitive information consistent with established OSMRE policies.
- (6) Reviewing and recertifying remote work arrangements on an annual basis to validate whether the arrangement is still effective and in the best interest of the agency.

E. **Remote Workers** are responsible for:

- (1) Providing the same level of support, availability, accessibility to customers,

coworkers, and supervisor as if working at the regular worksite. This includes, but is not limited to, meeting organizational and individual work requirements, participating in staff meetings, working assigned duty hours, and responding to phone calls, emails, and voicemail in a timely manner.

- (2) Ensuring there is no diminishment of individual performance or agency requirements.
- (3) Complying with their approved remote work agreement and adhering to Bureau policies while working at the remote worksite. These policies include, but are not limited to, Standards of Ethical Conduct for Employees of the Executive Branch and other applicable ethics laws and regulations, Acceptable Use of the Internet, Conduct and Discipline, Time and Attendance, and Records Management.
- (4) Properly protecting and securing GFE, agency records, and sensitive information in compliance with Bureau policies and guidance.
- (5) Ensuring the remote worksite is safe, free from hazards, and provides an adequate work environment regarding connectivity, technology, and privacy (as appropriate). Employees are expected to provide internet service and other general utility costs at their own expense.
- (6) Ensuring appropriate arrangements for the care of dependents while working from the remote location.