



COMMUNICATIONS PERSONNEL POLICY/PROCEDURE

Policy No. 1215	Date Issued: October 17, 2024
Section: 1200 – Personnel Policies	Date Revised:
SUBJECT: REMOTE WORK	
APPROVED:	<u><signed copy on file></u>
	Board Chairperson

1.0 Purpose

To provide guidance for supervisors and employees in establishing and maintaining remote work opportunities, when this work arrangement is appropriate and possible based upon the employee’s job duties.

2.0 Policy

Remote work opportunities offer supervisors and employees flexibility in determining the best way to meet operational needs. These arrangements can reduce driving and parking demands while optimizing workspace utilization at the Authority, allowing more efficient use of office space for on-site staff. Remote work is not a condition of employment; it can be requested by employees on a voluntary basis. Employees who are approved for remote work are expected to work a “hybrid” schedule which includes work on-site at the Authority for a minimum of two days per week, or more depending on operational needs. Generally, requests to work remotely 100% of the time will not be approved, barring exceptional circumstances. If a request for remote work is approved, a Remote Work Agreement is required. The agreement must be completed and signed annually by both the employee and employee’s supervisor.

3.0 Eligibility

Not every Authority position nor every Authority employee will be eligible to work remotely. The business needs of each division will determine eligibility. Even if the duties of a particular position can be performed remotely, not every employee in that position may be eligible to work remotely. Individual eligibility is at the discretion of the Division Manager and the General Manager.

Employees must be in good standing, meet job performance expectations, and comply with the terms of the Remote Work Agreement they make with their supervisor. Newly hired employees still in their initial probationary period are not eligible to request remote work.

At times, employees may also be required to return to work at the Authority site on their scheduled remote work days for operational reasons such as (but not limited to) meetings or staffing coverage.

3.1 Business Needs

The business needs of the Authority will be foremost in determining eligibility. Some jobs are not practical or possible to perform remotely. Each division will determine which positions and which employees are eligible for remote work.

Examples of work that can be performed remotely:

- Electronic correspondence
- Writing reports
- Meetings that do not require in person interaction
- Doing Authority business while accessing systems that are available remotely

Examples of work that needs to be done on site:

- Staffing reception desks
- Configuring or deploying computers or other physical equipment
- Performance evaluations, discipline, and grievance meetings
- Doing Authority business while accessing systems that are not available remotely

3.2 Geographic Work Location

The expectation is that employees who perform remote work will do so from their personal residence located in the state of California. This best ensures that the employee will be available to meet the County's operational needs, including reporting to the Authority work site if needed.

3.2.1 Remote Work Combined with Vacation or Other Leave

Remote work should not be combined with vacation or other absence from work. Exceptions may be granted with the advance approval of the Division Manager and the General Manager, under limited circumstances.

3.3 Remote Workspace and Environment

Employees working remotely must have a private, safe location to work. All standards for maintaining the confidentiality of information such as Personally Identifiable Information (PII) and Criminal Justice Information (CJI) must be in place. Policies that pertain to work environment and security at the Authority work site apply to the Remote Work site as well.

3.3.1 Confidential and PII Information

It is the duty of the employee to safeguard sensitive information, including PII, both while in the office and while working remotely. PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Examples of PII that are sensitive:

- Full or truncated Social Security numbers
- Dates of birth
- Addresses
- Phone numbers
- Email addresses
- Credit card numbers
- Financial information
- Mother's maiden name
- Biometric identifiers
- Medical information
- Passport number
- Driver's license number

CJI must be protected as described in the Criminal Justice Information Security (CJIS) manual. Employees accessing CJI are required to review requirements and pass an exam annually.

3.3.2 Documents

The employee and supervisor should work together to determine what types of documents are appropriate to take home and what documents should stay secured within the Authority workspace. Employees must ensure sensitive documents are appropriately marked and safeguarded to mitigate the risk of unauthorized disclosure.

3.3.3 Equipment and Document Security

The employee is responsible for securing Authority-related equipment and information, including while transporting information home or while traveling. If equipment or documents must be left unattended for a short period of time, always secure them, such as by locking the computer and putting documents away. Records must not be left unattended or exposed without proper safeguards. The employee's friends and family should not handle Authority records, so the employee must take care to put them away in a secure location. The employee should inventory documents prior to bringing them home and must ensure all documents are returned to the Authority workspace.

3.3.4 Communication

If other people are present at the employee's remote work location, then in addition to securing the computer and physical documents, the employee must also ensure that no one can overhear them when they are discussing confidential work matters over the telephone or in virtual meetings.

3.3.5 Ergonomics and Safety

The Authority will not set up or inspect the employee's remote workspace and it shall be the employee's responsibility to configure that space in a manner which allows them to perform their job duties safely and comfortably. If an employee is unable to set up their remote workspace in a manner which allows them to perform their work in a safe and ergonomically correct manner, remote work may not be appropriate for this employee.

The Authority is not responsible for any injuries that occur due to the employee's failure to set up the remote workspace in an ergonomically correct and safe manner.

3.4 Remote Work Agreements

Remote Work Agreements are negotiated between the employee and their supervisor. The agreement must contain details such as the employee's remote work location, work schedule, and any expectations that apply while the employee is working remotely. The Remote Work Agreement must be updated and signed annually.

4.0 Remote Work Expectations

Generally, the same productivity standards, performance expectations, accountability, and other policies shall apply to employees when working remotely as when working at the Authority work site.

4.1 Performance measurements

Supervisors will clearly communicate performance expectations to employees who work remotely and document and evaluate employees' compliance with those expectations. Supervisors should ensure work is completed correctly and in a timely manner, and that the employee receives appropriate training, guidance, and feedback. Performance evaluations shall be presented to the employee in person.

4.2 Communication

Supervisors will define communication standards and expectations and establish what status updates or check ins are required. The employee and supervisor should discuss the items listed below and document their agreement in the annual Remote Work Agreement.

4.2.1 Schedule

The employee and supervisor must establish a schedule that clearly specifies the hours and days the employee is working remotely and the hours and days the employee is working at the Authority work site. Employee schedules should be known to all employees which may be accomplished through use of the calendar system, the intranet website, and/or office whiteboards. The employee is responsible for reporting any changes to that schedule including absence and tardiness.

4.2.2 Authority business

Employees should be focused on and engaged in Authority business activities during their scheduled work time, regardless of where they perform that work. Employees will be accessible via email, phone, and other agreed-upon means of communication such as Teams or text messaging while working remotely and are expected to respond in a timely manner.

If employees who are working remotely need to conduct personal business during their scheduled work hours, they must do so during their meal and rest breaks or else make advance arrangements with their supervisor to adjust their work schedule to allow for the personal activities.

4.2.3 Work product/deliverables

The supervisor and employee must develop a plan for what work the employee will be performing while they are working remotely and specify how and when that work must be completed.

4.2.4 Feedback

Supervisors should conduct one-on-one and team meetings with employees working remotely with at least the same frequency as they conduct such meetings with on-site employees. Meetings may occur via virtual meeting applications, teleconference, or other remote communication methods. In addition to formal check-ins, supervisors should have regular communications with employees who are working remotely just as they would with employees who are working in the office.

4.3 Remote Meeting Attendance

Employees attending meetings while working remotely or who have requested remote attendance in advance, such as for meetings taking place outside of their normal in-office days/hours, are expected to be focused and engaged. Participation in meetings should not be combined with other activities that may distract the employee and prevent their full participation in the meeting.

Employees attending a meeting remotely must ensure they are in a quiet, distraction-free environment. The employee is expected to be on camera with audio and video enabled for the duration of the meeting. If the presenter has indicated they will be sharing materials that cannot be sent in advance, the employee must connect to the meeting using equipment that allows them to view

the materials. If an employee cannot meet these requirements, they must attend in person unless an exception is granted by the meeting facilitator and/or the employee's supervisor.

5.0 Equipment, Workspace, and Remote Work Environment

Most employees working remotely will require internet access, a computer, and a phone; other equipment may also be necessary. Departments will work with employees to determine an appropriate standard configuration for equipment and how the equipment needs will be met.

5.1 Internet Access

Employees accessing electronic tools, the Authority's network, and/or online Authority business applications will require reliable internet access that will allow them to perform their required job duties. Employees desiring remote work need to obtain, maintain, support, and pay for their own internet access.

5.2 Equipment

For most remote workers, computers, laptops, or tablets will be required to perform required job duties. Monitors, printers, webcams, headsets, and scanners are examples of other devices that might be required. The employee and their supervisor will work together to define the required tools and how they will be provided. This policy allows for the use of Authority-issued as well as personal equipment to be used by the remote worker.

5.3 Cybersecurity Requirements

Employees opting to use personal computers, laptops, or tablets that are used to access the Authority's network must have their own user name and password to the device that is not shared with other members of the household. In addition, they are required to install a remote management client provided by the Authority as well as an endpoint protection client. Questions about versions of operating systems, browsers, and other non-Authority supplied software may be referred to the Systems Division.

5.4 Systems Division Support

Systems Division staff are available to support remote staff. The Help Desk phone is staffed Monday through Friday, 8 a.m. to 5 p.m.. Email support is also available. Systems Division staff are not able to provide in-person services at the home of the remote worker. Systems Division staff are not responsible for supporting personal devices or other personal equipment, home internet services, or other non-Authority infrastructure used by the remote worker.

6.0 Compensation

Remote work is optional and working remotely does not change employee compensation. There is no differential for remote work. Employees working remotely who are required

to return to the Authority work location, or who are splitting their day between on-site and remote work, will not be compensated for travel, gas, or lodging.

7.0 Revocation of Remote Work

The Authority may rescind this policy at any time. The division manager or General Manager may determine that remote work is no longer appropriate for a position or that the employee is no longer meeting the eligibility requirements for remote work. This can be due to changes affecting or altering the employee's remote work site, employee performance issues, or other concerns. The responsibilities of the position may change, making remote work no longer appropriate. In any of these situations, the employee would be required to resume working exclusively at the Authority's work site.