t

Orlando College of Osteopathic Medicine

Policy Order Number: B012
Effective Date: October 25, 2024
Revised Date: October 25, 2024
BOT APPROVED: October 25, 2024

Robert T Hasty, DO, FACOI, FACP
Dean & Chief Academic Officer

**Policy Title: Remote Work Exceptions Policy**

**Policy Title:**
In-Person Work and Remote Work Exceptions Policy

**Policy Purpose:**
The purpose of this policy is to clearly define the expectations surrounding in-person work and the limited circumstances under which remote work may be authorized at Orlando College of Osteopathic Medicine (OCOM). This policy underscores the importance of on-campus presence in fostering a collaborative, student-centered environment that supports our institutional mission and vision. It also outlines the procedures for requesting and authorizing remote work, ensuring that any temporary arrangements align with our commitment to team cohesion and student success.

**Policy Statement:**
At OCOM, we believe that an in-person work environment is essential to building a strong, connected team that upholds our values of student-centered education. Being physically present on campus enhances collaboration, communication, and the overall work culture, all of which are integral to achieving our mission of supporting student success.
Remote work will only be considered in rare and exceptional cases where it is necessary for short-term needs. These situations will be evaluated individually, and

remote work will only be approved on a temporary basis. All employees are expected to adhere to this policy to maintain the effectiveness of the institution and contribute fully to the in-person work environment.

While we recognize that remote work may occasionally be necessary due to unforeseen circumstances, such instances will be considered an exception - rather than the norm. The following principles guide our remote work policy:

- **On-Campus Work Requirement:** All employees are required to work on campus to contribute to the vibrant campus environment that supports our institutional goals. In person presence is foundational to building relationships, enhancing teamwork, and providing the best possible experience for our students.
- **Temporary Remote Work Exceptions and Revocations:** In rare and exceptional cases, remote work may be authorized on a temporary basis. Such arrangements will be evaluated on a case-by-case basis and must receive prior approval from the employee's Department Leader with a final approval from the Dean/CAO or President. Remote work approval will only be granted for a specified, temporary period, and requests for remote work require clear justification. Not all roles will be eligible for remote work. Department Leaders will continue to review work location arrangements and make changes as warranted by institutional needs. If a Department Leader, the Dean/CAO, or President deems that a remote work arrangement is not suitable for a person/role/department, the remote work arrangement can be revoked at any time.
- **Authorization and Tracking:** Requests for temporary remote work must be submitted in writing and pre-approved by the Department Leader and submitted to the Dean/CAO or President for final approval. Once approved, these arrangements will be reported to Human Resources to ensure tracking and compliance with institutional policies.
- **Expectations for Remote Work:** If remote work is authorized, employees are expected to maintain productivity through virtual meetings, email, and other communication methods. Regular updates and check-ins are required to ensure that remote work does not compromise performance or team collaboration.
    - **Workspace:** Employees authorized to work remotely must create and designate an appropriate working environment for their remote work location. During established work hours, this workspace should be quiet and free from distractions so that they can dedicate their full attention to their job duties. Working in public places or spaces, use of public

networks, and/or working in a location where screens may be visible to others are prohibited.

- **Work Hours**: Department Leaders will collaborate with authorized employees to establish regular work hours (e.g., 9:00 a.m. – 5:00 p.m.). During these work hours, employees must be available, accessible, and responsive in the same manner they would be if they were in the office and on-campus. Department Leaders will establish communication expectations with remote workers including preferred methods of communication, including but not limited to regular updates to be provided, reporting of work hours, and daily check-ins.

- **Dependent care**: Remote work is not intended to be a replacement for childcare or care of other dependents. Remote workers are expected to make arrangements for care of dependents and personal needs during work hours, just as they would if they were working on campus.
- **Equipment and Technology:** Before beginning remote work, eligible employees should confirm with their Department Leader and IT that they have all required and OCOM-issued hardware, software, and passwords and that they have established access to the OCOM network and other systems as needed.
- **Data and Internet Security**: Remote workers must adhere to the following requirements:
    - Remote workers must use OCOM-issued laptops and/or desktops, as opposed to personal devices, for remote work, unless they receive prior written approval from their Department Leader and IT.
    - When not in use, remote employees must store OCOM-issued device(s) in a secure area.
    - Employees may not permit unauthorized users to access or operate OCOM-issued hardware, software, networks, systems, or passwords.
    - Employees shall take reasonable precautions to prevent unauthorized access to their work devices and systems without their knowledge, including locking their remote laptop/desktop whenever stepping away for any period of time.
    - Employees should report any suspicious activity on their remote laptop/desktop to a member of IT for investigation, escalation, and/or resolution. This could include, for example, files becoming encrypted, deleted, or moved; increased frequency of pop-ups while browsing the internet; or new applications being installed.

- Employees must not, under any circumstances, deactivate security software on OCOM-issued/owned devices.
- In addition to the above requirements, employees must at all times abide by the Acceptable Use Policy.

- **Non-Compliance:** Failure to comply with this policy, or failure to meet the work requirements while working remotely, may result in corrective action, including performance improvement plans or potential termination of employment.

**Review and Revision:**

This policy will be reviewed regularly by the ***Policy Review Committee*** to ensure it remains aligned with institutional goals and evolving work needs. Any amendments or changes will be communicated to all employees accordingly.