Telecommuting Policy

Effective Date: March, 2019
Revised: November, 2021

Office: Human Resources, Information Technology, Office of General Counsel & Risk Management

PURPOSE:

This policy is intended to provide guidance for telecommuting arrangements for employees.

REFERENCE DOCUMENTS/ RELATED INFORMATION:

Extreme Weather Policy

Telecommuting Policy FAQ

SCOPE:

All Staff

Telecommuting: a work arrangement where an employee performs his/her usual job duties from another location away from the usual workplace.

POLICY STATEMENT:

With prior approval, employees, whose job responsibilities are suitable for telecommuting, can complete part or all of their normal business day from another location away from the usual workplace. Telecommuting requests, for non-location critical positions, may be approved with the following guidelines:

General Guidelines:

- The University may, in its sole discretion, restrict or revoke telecommuting privileges at any time.
- No University employee is entitled to or guaranteed the opportunity to telecommute.
- Some positions may not be eligible for telecommuting due to the nature of the employee's work. Eligibility will be determined by supervisors.
- Telecommuting requests must be approved *in advance* by the employee's supervisor.
- Frequency and regularity of an employee's telecommuting will be determined by supervisors.
- The supervisor determines work to be performed and documentation of time spent may be requested.
- The employee *must* be reachable during normally scheduled working hours by phone, email, text, chat just as if the employee was in the office in person. It might be necessary for calls to be forwarded to a cell phone in order to successfully telecommute.
- If the employee routinely receives business phone calls throughout the work day, he/she should plan on checking voicemail frequently.
- Supervisors and managers may cancel a pre-approved telecommuting day if required for operational/business needs, special events, or emergencies.
- Because telecommuting is a privilege, University management reserves the right to review any telecommuting arrangement at any time in light of employee performance as determined by the following factors: 1) quality of employee work product; 2) efficiency with which an employee delivers work product in accordance with assigned deadlines; 3) the employee's ability to support student/customer/client needs and provide follow-up on a timely basis; and 4) the employee's ability to meet management expectations with respect to overall job performance.
- Anyone found abusing this privilege may lose future opportunities to telework and face other disciplinary actions up to and including termination. Decreases in productivity or behaviors that detract value from the University may result in the immediate loss of telecommuting privelege and/or may result in disciplinary action.
- This policy is not intended to replace the University's sick or vacation leave policies.
- Telecommuting time is not a leave time benefit subject to accrual or payout at any time.
- Telecommuting should not be used to provide active care for a child or other dependent.
- An employee's classification, compensation, and benefits will not change if the employee is approved to telecommute.
- Overtime is prohibited while telecommuting

Process for Telecommuting Request & Criteria for Supervisor/Manager Decision:

- A supervisor determines whether an employee is a good candidate for telecommuting. (Consider factors such as, but not limited to, completion of the probationary period, satisfactory performance, and the ability to work independently).

- Supervisor should also consider that certain positions like those below do not lend themselves to telecommuting. Typically, it will be positions that require minimum physical activity, low overhead, definable and measurable goals, and long-term deadlines.
    - The following conditions make telecommuting unsuitable: equipment, materials, and files necessary to the position can only be physically accessed on University property
    - Face-to-face contact with supervisors, other employees, clients, or the public on University property is a regular and integral part of the position responsibilities
    - In addition, despite the suitability of positions or employees to telecommuting arrangements, departments must ensure that sufficient personnel are available on campus to provide service to the campus community during scheduled business hours. As a result, there may be limited opportunities for employees to make use of telecommuting arrangements
    - When determining whether telecommuting is compatible with certain jobs, supervisors should assess data security issues that might arise from telecommuting. Supervisors are encouraged to consult with Information Technology if questions arise.
- Determine that the nature of work is suitable for performance from a remote site.
- Evaluate and consider how the proposed arrangement will impact other employees or the department as a whole.
- The supervisor determines and communicates if the telecommuting request is denied or granted.

Important Requirements and Considerations:

Costs: The University will not pay for or reimburse any costs associated with telecommuting. Charging telecommuting expenses to a University credit card is strictly prohibited. This includes, but is not limited to, costs associated with an internet connection, equipment, landline or mobile phone, etc. Any employee opting to work remotely who is also unwilling or unable to cover the costs associated with telecommuting should report to work at his/her regular work space and use University-provided services and equipment.

Work Space: The location from which the employee will telecommute should have the necessary equipment for the employee to perform the requirements of the position. Further, the location should be one that will not interfere with the employee's participation in telephone or video meetings or lead to the inadvertent disclosure of confidential or proprietary information to third parties at the telecommuting site.

According to the Occupational Safety and Health Administration (OSHA), there is no provision in the law that excludes workplaces located in a home. Because of this, employees working from home should take reasonable steps to ensure that the work environment is safe and free from hazards. Employees should also be familiar with Worker's Compensation procedures.

When working at home or elsewhere, the employee is responsible for establishing a work environment free of interruptions and distractions that would affect performance. The employee is also responsible for any ergonomic needs that an employee may have in a home office.

IT Support: University staff cannot provide hands-on assistance for any equipment or connectivity issues to employees working remotely outside the university. The University's Information Technology Staff may be able to access university-owned computers remotely to resolve issues. If that is unsuccessful, the employee may need to bring the computer to campus for troubleshooting, repairs, or replacement. IT support will be best-effort for non-UIndy owned devices or older platforms that may be unsupported by the vendor or by the software manufacturer.

Support for a network connection to the University is strictly limited to establishing a connection through the University's virtual private network (VPN). Information Technology staff will not provide support for an individual's home network, wifi or internet service. Operating system, software or configuration issues that prevent the installation of the University's virtual private network (VPN) cannot be supported.

Visit the Information Technology FAQ for more information about connecting to the UIndy VPN.

MacOS – http://technology.uindy.edu/faq/content/1/470/en/how-do-i-connect-to-the-uindy-vpn-mac-os-x.html?highlight=vpn

Windows - http://technology.uindy.edu/faq/content/1/469/en/how-do-i-connect-to-the-uindy-vpn-windows.html?highlight=vpn

Telecommuting Technology and Information Security Guidelines: Concerning a remote working environment, the employee will be responsible for complying with all University policies and guidelines. The employee working remotely is responsible for protecting the University's data and systems that are both remote and those accessed remotely that are located at University facilities.

For working remotely, it is the employee's responsibility to follow the same best practices for protecting physical and electronic information and resources as is required at all University locations. The employee must ensure the physical security of the equipment used to access UIndy information and resources. This includes protecting University information and remote-working equipment from being stolen or accessed by unauthorized persons. This also includes the security of information in paper format including ongoing storage, back-ups, and proper disposal. Hardware, software and data destruction of confidential materials must be done securely and disposed of at the termination of business need. Remote working arrangements should be equipped to facilitate this activity (a cross-cut shredder) or include the employee bringing materials to UIndy to be disposed of through standard on-site processes.

Users may not store any University confidential or personally identifiable information (PII) data on their personally owned laptop. Any storage or processing of confidential or personally identifiable information (PII) should be done only on a University Supplied laptop. Employees are to safeguard student, employee, and other customer information by turning off or removing from the work area devices such as Amazon Alexa and Google Home.

FERPA and Other Confidentiality Requirements and Considerations: Employees remain subject to all FERPA and University confidentiality requirements while telecommuting. Employees are reminded of their obligation to protect the University's proprietary information at all times regardless of where they are working, and to be mindful of confidentiality considerations when telecommuting in a public place away from their regular work space. Employees are *strongly* discouraged from taking paperwork and

documents bearing any FERPA or confidential information on them home or to a telecommuting location. If, however, the employee is required to take any such paperwork or documents for use when telecommuting by a supervisor, the employee is required to keep all items secure and safe from inadvertent disclosure, including through loss or destruction.

If sensitive data is lost or stolen, please report the theft immediately to the University Risk Manager.