

HR 90 — Telecommuting

<p>Purpose and Objectives</p>	<p>The Wisconsin Department of Revenue recognizes the potential value and benefit of telecommuting as an option to achieve its mission, although telecommuting will not generally be appropriate for managers, attorneys, employees in positions that work directly with taxpayers or sensitive taxpayer information, and staff who support those positions. Employees who travel extensively for their jobs may be exceptions to this rule. The operational needs of the Department will be the primary consideration in reviewing requests for telecommuting.</p>
<p>Defined</p>	<p>Telecommuting means working, on a regular basis, away from an established DOR office, using either the home or an alternative site as the base of operations.</p> <p>Telecommuting is a formal, scheduled work location alternative that allows employees to meet customer needs by performing job responsibilities away from an assigned DOR office. Homes or alternative work sites of telecommuting employees are equipped with information technology that is appropriate for the tasks being performed.</p> <p>Telecommuting relates to employees who work partially at an assigned DOR office, AND work partially at home or at an alternative site those who work at home or at an alternative site full-time; and those who are mobile workers, that is, those who travel continuously or frequently and return to an office in their home.</p> <p>It does not apply to employees who:</p> <ol style="list-style-type: none"> 1) are mobile workers, that is, those who travel continuously or frequently and return to their assigned DOR office, or 2) who work at home on a short-term basis, or 3) who work at home as either a temporary or permanent reasonable ADA accommodation or Return to Work program, or 4) who work at home as part of the Department’s plan for response to emergency or pandemic situations.
<p>Security</p>	<p>DOR <u>Policy 110-14 (IT 34)</u> Minimum Electronic Data Security is the operative policy. It provides that “All DOR Information system policies apply anytime DOR data networks, or hardware are used whether on or off site.”</p> <p>Only Department-owned computers and software may be used to process, access and store confidential taxpayer data, personnel, or other sensitive Departmental information. (Policy 110-7 [IT</p>

	<p>14]) DOR-owned Computer Software on Employee-owned Devices.) The Department retains ownership and control of all hardware, software, telecommunication equipment and data placed in the homes or in alternative work sites of employees.</p> <p>Taxpayer information may be stored on hard disks (H:\ Drive or home directory) only if agency-approved security access control devices have been installed. The home directory (hard disk) is not considered the final resting place for any business-related data. (See Policy 110-12 [IT 33] y) Electronic Data Management.)</p> <p>Access control must include password security, an audit trail, encryption, virus detection, and data overwriting capabilities. (See Policy 110-5 [IT 31]) Data Access Policy.)</p> <p>All electronic information must be encrypted before storage and decrypted only at its destination point of use. (See Policy 110-11 [IT 32] y) Data Storage and Transport Policy.)</p> <p>All connections between DOR private internal networks and the Internet (or any other publicly accessible computer network) must go through DOR firewalls and related access controls such as Logon Id/Password or Digital Certificate. (See Policy 110-4 [IT 30]) Access and Firewall Policy.)</p> <p>Information technology storage devices used for DOR equipment or data must be issued by DOR, may only be used for DOR-authorized purposes, and must be stored in a secure location when not in use. (See Policy IT 15, Information Technology Storage Devices.)</p>
<p>Safeguarding Computers</p>	<p>Computers may not be left unprotected at any time by the employee. If an employee is interrupted in their work or leaves the computer, the employee will invoke the password-protected Microsoft Windows Security feature “Lock Computer”.</p> <p>Access to the computer must be restricted to DOR employees.</p> <p>DOR-owned data, software, and equipment may not be used by anyone other than the approved telecommuting employee for approved use.</p> <p>Telecommuters may not have DOR business meetings or DOR-related or unrelated visits from any non-DOR employee in their telecommuting work space, other than inspections related to telecommuting eligibility.</p>
<p>Secure devices</p>	<p>The Department will provide telecommuting employees with the necessary personal computers or laptops, pre-loaded software, encrypted electronic storage devices, locking file cabinets, paper shredders, and such other equipment as may be necessary so that documents, disks, tax returns, etc., may be properly secured when not in use.</p> <p>All confidential records must be stored in a locked cabinet used</p>

	<p>exclusively for DOR business when not in use. Confidential records must not be viewable by non-employees in the telecommuting work space. Confidential records that are no longer needed must be returned to the DOR headquarters office for record retention or destruction or destroyed in DOR provided equipment.</p> <p>The agency will provide locking hardware to secure Automated Data Processing equipment to large objects such as desks or tables. Smaller DOR-owned equipment, particularly laptops, must be locked in a DOR-only filing cabinet or dedicated desk drawer when not in use.</p> <p>Employees must have a dedicated area that has the appropriate space and facilities for the type of work done and must have two barriers to access confidential taxpayer information – a locked perimeter and locked interior.</p> <p>The Department assumes no liability for loss, damage, or wear of employee-owned equipment. Any software, products, or data created as a result of work-related activities are the property of the Department.</p>
<p>Eligibility</p>	<p>An employee is eligible to telecommute when his or her telecommute request meets the needs of the Department, and:</p> <ol style="list-style-type: none"> 1. The employee has permanent classified or unclassified civil service status, is not on any probationary period, and is; <ul style="list-style-type: none"> • at the development level of their classification if, in the judgment of management, approval will benefit the Department or • at the objective level of their classification specifications, and 2. The employee has a demonstrated record of punctuality, attendance, effective work habits, and excellent productivity and performance, with no significant disciplinary issues as evidenced by an accurately completed <i>Telecommuting Eligibility Checklist</i>, and 3. The duties of the position can be performed remotely, as evidenced by the completed Telecommuting Eligibility Checklist, and 4. The job duties of the position do not require regular contact with taxpayers, other DOR staffers or other members of the public at a DOR office, <p>Any one of the above four numbered requirements may be waived if telecommuting is a condition of employment for an employee that does not have permanent civil service status or if the employee's job description requires telecommuting and their position, skills, and abilities conform to specified assessment considerations outlined in the <i>Telecommuting Eligibility Checklist</i></p>

	<p>found in the Appendices.</p> <p>A request to telecommute may be initiated by the employee or by the Department. An employee may turn down a request to telecommute without harm to his/her performance review or personnel record.</p> <p>Costs associated with a telecommuting request, including the installation of necessary equipment, will be reviewed as part of the approval process.</p>
<p>Telecommuting plan</p>	<p>If telecommuting is determined to be a viable work option, employees are responsible for working with their manager/supervisor to develop an acceptable telecommuting plan.</p> <p>The plan will distinguish between telecommuters who will be handling confidential taxpayer data, personnel, or other sensitive Departmental information and those who will not be. Telecommuters who will be handling confidential or sensitive Departmental information must agree to abide by each of the Department's data security, access, firewall, storage, data management policies, and space requirements.</p> <p>The specific telecommuting schedule (hours and days), location, duties, and methods of contact to be used by a telecommuting employee will be documented in a written plan to be signed by the employee and his/her supervisor. Managers may have specific needs related to work functions and will document them in the plan. The plan must address all considerations mentioned in this policy.</p> <p>The plan may specify the duration of telecommuting. The plan must be signed by the employee, immediate supervisor, and approved by their division administrator or designee and by the human resource director.</p> <p>Any change in the agreed-upon schedule must be approved by the manager/supervisor prior to implementation. The plan must be reviewed at least annually and signed by the manager and the employee.</p> <p>The Department reserves the right to access the telecommuter's work site during working hours.</p> <p>An agreement to telecommute is not transferable to other positions within the Department and may be terminated by the Department at any time, provided two weeks notice is given to the employee, or without notice if there is just cause for such termination.</p>
<p>Employee responsibility</p>	<p>All Departmental work rules and policies, including the <u>Confidentiality/Anti-Browsing Policy</u>, remain applicable.</p> <p>Employee compensation, benefits, work status, rights, and work</p>

	<p>responsibilities do not change due to participation in the Telecommuting Program.</p> <p>The amount of time the telecommuting employee is expected to work per pay period does not change.</p> <p>The telecommuting employee must:</p> <ul style="list-style-type: none"> ▪ Submit a written request to telecommute to their manager/supervisor. If telecommuting is determined to be a viable work option, the employee is responsible for working with his or her manager/supervisor to develop an acceptable telecommuting plan. ▪ Get remote access approval Form ASC-520. ▪ Use only DOR-provided software on DOR-owned computer equipment. ▪ Notify their manager/supervisor and the Help Desk immediately in the event of equipment malfunction or security breach. ▪ In the case of a security breach, immediately disconnect and power down all information technology devices. ▪ In the case of an equipment malfunction, take the equipment to a site designated by the Department for repair. ▪ Adhere to all DOR policies and state statutes regarding security and the appropriate use of state equipment. ▪ Provide methods of contact, including back-up and emergency contacts. ▪ Take personal leave time if he or she performs family care, housekeeping, etc. during work hours. ▪ Be accessible via telephone, answering machine, voice mail, pager, e-mail, etc. ▪ Attend all assigned office meetings. ▪ Forego telecommuting if directed to report to the assigned DOR office.
<p>Supervisor responsibility</p>	<p>Managers and supervisors are responsible for the administration of telecommuting in their area of responsibility, including:</p> <ul style="list-style-type: none"> ▪ Determining whether an employee and his or her position are suitable for participation in the telecommuting program. ▪ Determining whether an employee's request to telecommute will contribute to the department's goals, including reducing costs, increasing productivity, and providing good customer service. ▪ Determining and inventorying the use of DOR-owned equipment.

	<ul style="list-style-type: none"> ▪ Approving/disapproving the use of non-DOR-owned equipment. ▪ Recovering DOR-owned equipment at the conclusion of a telecommute period. ▪ Monitoring the day-to-day performance of employees as they would any other employee.
Office of Technology Services	<p>The Office of Technology Services (OTS) is responsible for:</p> <ul style="list-style-type: none"> ▪ Approving the remote access request. ▪ Determining computer hardware, software, and related equipment needs.. ▪ Facilitating the acquisition and installation of information technology hardware and/or software and related equipment.. ▪ Arranging for the removal of DOR-owned equipment from the telecommuting employee's home or alternative site when telecommuting is discontinued.
Authorized Expenses	<p>Telecommuting employees must use supplies available through their division or office whenever possible. Any telecommuting expenses not specifically covered in these guidelines will be considered on a case-by-case basis by the manager/supervisor.</p> <p>The Department of Revenue will pay the following expenses:</p> <ul style="list-style-type: none"> ▪ Normal maintenance and repairs to DOR-owned equipment, by a state-approved vendor. ▪ Software required for assigned work. ▪ Charges for a second telephone line installation (DOR will not pay for laying a new telephone line from street to house). ▪ The cost of computer supplies and the monthly charge for a dedicated second telephone line at the home office. ▪ Business-related telephone and fax calls. ▪ Business-related charges for photocopying, mailings, and package delivery. ▪ Some business-related travel from the home or other alternative work site (e.g., travel to/from neighborhood fax and copy centers). ▪ Post Office boxes for business mail. ▪ High-speed Internet access. <p>Claims for reimbursement must be approved in advance by the manager/supervisor for single purchases over \$25. Purchases must follow standard DOR purchasing rules and procedures.</p> <p>Workers' Compensation laws and rules will apply to an employee's work-related injury while telecommuting. The</p>

	<p>employee must notify their manager/supervisor immediately and complete all necessary and/or management-requested documents regarding the injury.</p>
<p>Non-reimbursable expenses</p>	<p>The telecommuting employee is responsible and holds the Department harmless for the following expenses:</p> <ul style="list-style-type: none"> ▪ Maintenance and repairs of privately owned equipment. ▪ Any electrical and/or utility costs associated with the use of equipment in the home. ▪ Travel expenses associated with commuting to the employee's assigned office. ▪ Office or equipment supplies that the employee would normally acquire from the employee's central office (unless approved in advance by the manager/supervisor). ▪ Any costs associated with the employee's own furnishings in the home office, including, but not limited to, insurance, furniture, locks, and equipment. ▪ Expenses for reconfiguring a home office if telecommuting is terminated. ▪ Injuries sustained by employees, their family, or third parties using non-Departmental equipment. <p>The Department of Revenue is not responsible for substantiating employees' claims of tax deductions for operating offices within their homes.</p> <p>The Department is not liable for damages sustained in the home or other alternative telecommuting environment except as may result from the use of Revenue-owned equipment in the course of the employee's duties.</p>
<p>For more information:</p>	<p>See also:</p> <ul style="list-style-type: none"> ▪ IRS Publication 1075 Tax information Security Guidelines for Federal, State and Local Agencies ▪ Telecommuting Guidelines, State of Wisconsin DOA. Includes ergonomic suggestions for the home office. ▪ Employee's Guide to A Proper Telecommuting Environment ▪ Telecommuting Plan and Attachments

Contact: Human Resource Director

Updated: May 20, 2008